

**Caro Leitor,**

Há alguns meses, quando decidimos lançar uma revista técnica, com a chancela da Prodemge, estabelecemos de imediato um compromisso: criar uma publicação relevante, que tivesse um destino outro que enfeitar mesinhas de ante-salas de repartições. O maior temor num projeto como esse era de que, depois de pronto, soasse como uma mera reverência às vaidades de uma estatal que atua no ramo da tecnologia.

Definimos então, como premissa editorial, a concentração exclusiva em temas que estivessem na ordem do dia dos usuários, atuais ou potenciais, da tecnologia da informação. Além disso, a abordagem deveria buscar o tom exato entre a profundidade e a leveza. A primeira, deveria torná-la referência de pesquisa para usuários, técnicos e executivos em busca de conhecimentos para ajudá-los em suas decisões e estudantes em busca da última palavra sobre os temas em pauta. A segunda, cuidaria de que fosse uma publicação agradável, rica e informativa, capaz de despertar também a atenção do público interessado, mas não especializado, importante já que numeroso e formador de opinião.

Este primeiro número de Fonte reflete bem essas diretrizes.

O tema não poderia ser mais atual: Certificação Digital.

É assunto novo, com vastas áreas ainda em discussão, e que certamente provocará, em futuro próximo, profunda revolução nos costumes da sociedade em geral e, principalmente, na administração pública, com reflexos simplificadores sobre a vida dos cidadãos. Abordamos todos os seus aspectos: os legais, os técnicos, os administrativos e os culturais. Buscamos como colaboradores as maiores autoridades em cada setor, que contribuíram com entrevistas exclusivas ou textos inéditos. Procuramos, sem a pretensão de esgotar o assunto, refletir o panorama mais atual do estágio em que se encontram as discussões sobre o tema no País.

Temos a consciência de que o que apresentamos agora não é um produto acabado. Por isso, abrimos uma seção para interação com os leitores. Dela, tiraremos sugestões, ouviremos críticas e, eventualmente, buscaremos inspiração para possíveis e oportunas correções de rumo.

Finalmente, analisando este primeiro número de Fonte, que agora publicamos, temos a esperança de termos escapado da irrelevância.

No entanto, submetemos esta avaliação ao julgamento soberano - na realidade o que realmente importa - dos nossos leitores.

Um abraço,

**Maurício Azeredo Dias Costa**

Uma Publicação da:



Ano 1 - nº 1 - Dezembro de 2004

**Governador do Estado de Minas Gerais**  
Aécio Neves da Cunha  
**Secretário de Estado de Planejamento e Gestão**  
Antonio Augusto Junho Anastasia  
**Diretor-Presidente**  
Maurício Azeredo Dias Costa  
**Diretora de Projetos e Negócios**  
Glória Maria Menezes Mendes Ferreira  
**Diretor de Tecnologia e Produção**  
Raul Monteiro de Barros Fulgêncio  
**Diretor Administrativo e Financeiro**  
José Ronaldo Fidelis  
**Diretor de Desenvolvimento Empresarial**  
Nathan Lerman

## Fonte

### CONSELHO EDITORIAL

Antonio Augusto Junho Anastasia  
Maurício Azeredo Dias Costa  
Márcio Luiz Bunte de Carvalho  
Amílcar Vianna Martins Filho  
Gustavo da Gama Torres  
Paulo Kléber Duarte Pereira  
Marcos Brafman

### EDIÇÃO EXECUTIVA

Assessoria de Comunicação  
Pedro Marcos Fonte Boa Bueno  
Edição, reportagem e redação  
Isabela Moreira de Abreu - MG 02378 JP  
Coordenação do projeto editorial, gráfico e publicitário  
Gustavo Grossi de Lacerda  
Universidade Corporativa Prodemge  
Enilton Rocha Ferreira  
Marta Beatriz Brandão P. e Albuquerque  
Luiz Cláudio Silva Caldas  
Projeto gráfico, capa, ilustrações, diagramação  
e editoração gráfica  
Guydo José Rossi Cardoso de Menezes  
Estágio programação visual  
Camila Maciel Leite Seabra  
Revisão  
Fátima Campos  
Fotolito e impressão  
Policron / Gráfica Formato  
Tiragem  
Três mil exemplares  
Periodicidade  
Semestral

### PATROCÍNIO

Esta edição da revista contou com o apoio:



**Prodemge - Rua da Bahia, 2277 - Bairro Lourdes  
CEP 30160-012 - Belo Horizonte, MG, Brasil**  
[www.prodemge.mg.gov.br/](http://www.prodemge.mg.gov.br/) / [prodemge@prodemge.gov.br](mailto:prodemge@prodemge.gov.br)



**Fonte**

---

# Sumário

---

**Fonte**

Número 01 - Dezembro de 2004

**prodemge**

Tecnologia de Minas Gerais

---

- 03** **Interação:** comentários e sugestões de leitores
- 04** **Diálogo:** entrevista com o advogado-geral do Estado de Minas Gerais, José Bonifácio Borges de Andrada, que fala dos aspectos histórico e jurídico da certificação digital no País
- 11** **ICP-Brasil: Evolução com Equilíbrio e Correção** - o diretor do ITI, Evandro Oliveira, aborda o comportamento do mercado frente à consolidação da certificação digital
- 13** **Governo Eletrônico: Projeto de Segurança da Informação do Governo Mineiro** - a secretária-adjunta de Planejamento e Gestão do Governo do Estado de Minas Gerais, Renata Vilhena, comenta o desafio da segurança da informação com o uso crescente da tecnologia
- 14** **A Criptografia na Ficção** - técnicas antigas e fantasias modernas no artigo do analista de sistemas da Prodemge, Luís Carlos Silva Eiras
- 16** **Dossiê:** panorama da certificação digital - aplicações, benefícios, perspectivas e a opinião de autoridades no assunto
- 32** **Benchmarking:** duas experiências de sucesso - a Receita Federal e o Tribunal Regional do Trabalho 4ª Região (RS)
- 35** **Fórum:** a certificação digital e os cartórios - o professor de Ciência Política, José Eisenberg, comenta o desafio que a certificação digital representa para o futuro da burocracia
- 37** **Universidade Corporativa Prodemge:** seleção de artigos acadêmicos inéditos sobre os temas certificação digital e segurança da informação
- Considerações sobre a interoperabilidade aplicada à infra-estrutura de chaves públicas - Fabiano Menke
- A privacidade na ICP-Brasil - Alexandre Rodrigues Atheniense
- Tudo que você deve saber sobre certificação digital - Jeroen van de Graaf
- Certificação digital: uma realidade em Minas - Raymundo Albino e Sérgio Daher

---

# Interação

---


Este espaço é  
destinado a acolher  
as opiniões e  
sugestões de  
nossos leitores.

Participe, contribua,  
faça contato:  
seu retorno é  
fundamental para  
que a  
revista evolua a cada  
edição.

---

**e-mail:**  
**[revistafonte@prodemge.gov.br](mailto:revistafonte@prodemge.gov.br)**

---



Rua da Bahia, 2277, Lourdes -  
Belo Horizonte, MG - CEP:  
30160-012, aos cuidados da  
Assessoria de Comunicação da  
Prodemge - Companhia de  
Tecnologia da Informação do  
Estado de Minas Gerais.

### Segurança e armazenamento de documentos: da inscrição na pedra à Certificação Digital



**José Bonifácio Borges de Andrada, advogado-geral do Estado/MG. Dentre os vários cargos públicos que exerceu, foi advogado-geral da União, subsecretário-geral da Presidência da República, secretário-executivo do Ministério da Justiça, subchefe para assuntos jurídicos da Casa Civil da Presidência da República e consultor jurídico do Ministério da Previdência e Assistência Social. Tem o cargo efetivo de procurador regional da república.**

Na primeira edição da Revista Fonte, o entrevistado é o advogado-geral do Estado, José Bonifácio Borges de Andrada. Com larga experiência no setor público, no qual ocupou importantes cargos nos governos Federal e Estadual, e também com grandes conhecimentos na área de tecnologia da informação, o advogado-geral do Estado teve participação decisiva na criação da Infra-Estrutura de Chaves Públicas do Brasil – ICP-Brasil, atuando primeiramente como consultor jurídico do Ministério da Previdência e Assistência Social, onde surgiram as primeiras evidências da necessidade de mecanismos de proteção às informações eletrônicas; e, posteriormente, como subsecretário-geral da Presidência da República e advogado-geral da União, quando foi finalmente estabelecida a Medida Provisória 2200, que regulamenta a certificação digital no Brasil.

Nesta entrevista, José Bonifácio traça, de forma didática, um panorama histórico da certificação digital no País e fala, com propriedade e bom humor, das perspectivas dessa tecnologia no Brasil. Ele refuta o mito de seu uso explosivo no comércio eletrônico e pontua os benefícios de sua utilização para o setor público, enfatizando a experiência em Minas, onde a tecnologia tornou-se realidade em 2004.

**Fonte: Como surgiram as primeiras iniciativas para estabelecer o serviço no Brasil?**

“Eu fui despertado para essas questões de informática, do ponto de vista legal, quando trabalhava no Ministério da Previdência. Algumas fraudes vinham sendo feitas no sistema ou através do sistema. Algumas, muito primárias, muito simples; outras, devido à falta de cuidado de pessoas que deixavam seu cartão magnético com a senha pregada com durex na tela do computador, para facilitar o serviço. Havia no entanto outras mais complexas, mais elaboradas, que exigiam um pouco mais de conhecimentos. Houve um dia em que um hacker conseguiu fazer clone da página da Previdência e colocou informações para confundir as pessoas. A nossa sorte é que ele colocou um Fale Conosco. Mandamos então um e-mail para ele, dizendo que a Polícia estava chegando. Conseguimos resolver o problema e tirar a falsa página do ar.

Com esses episódios, chegamos à conclusão de que era necessária uma legislação criminal específica para a área previdenciária. Elaboramos então algumas alterações no Código Penal, que estão em vigor hoje, para a proteção da base de dados da Previdência. Esse projeto foi encaminhado ao Congresso. Nesse meio tempo, eu fui convidado para trabalhar na Casa Civil e o projeto tramitava no Congresso.

Na Casa Civil, nós temos um contato maior com a estrutura de Governo e começamos a perceber que a demanda era comum a todos os outros órgãos.”

**Fonte: Naturalmente, houve necessidade de adequações na Lei. Como foi conduzido o processo?**

“Percebemos que todos os órgãos tinham dados e informações que precisavam ser preservados e que o projeto da Previdência, que estava mais avançado, na verdade servia para todo mundo. Fizemos então algumas alterações no Projeto de Lei que estava na Câmara e o adequamos para a administração pública. Foram então criados, pela primeira vez, alguns crimes específicos, que estão no Código Penal. Isso é importante também: não fizemos uma lei específica, fizemos alterações no Código Penal, que é a lei penal comum, que todo mundo usa, a lei básica criminal do País, protegendo documentos e informações constantes em bases de dados e também criando algumas hipóteses criminais de invasão de bases de dados.

Por exemplo, ceder senha de acesso a um banco de dados protegido a um terceiro, em certos casos, é crime. Uma pessoa não pode passar informalmente a senha a uma pessoa não autorizada. Só passar a senha já é crime. Se isso significa uma invasão a uma base de dados, é um outro crime com pena mais grave. Se, da invasão, resulta um dano à base de dados, aí é outro crime, com pena mais alta ainda. Não estávamos ainda na fase da certificação digital. Mas chegou-se a um ponto em que houve demanda pela certificação digital.”

**Fonte: Nessa época, como outros países conduziam a questão da segurança de seus documentos eletrônicos?**

“Nessa época, ou um pouquinho antes, a Europa já tinha feito uma diretriz para a União Européia. Uma diretriz básica que orientava todos os países sobre como regulamentar a certificação digital na Europa.

Outros países também estavam fazendo uma legislação própria. Nos Estados Unidos, bem no seu estilo – devido à liberdade de cada Estado –, cada um definia

**“Foram estudados os modelos do mundo e o governo optou por adotar o modelo vigente na Comunidade Européia...”**

sua forma de atuação mais conveniente. Mas o assunto estava em fase de organização, por volta de 1999/2000.

E nós sentimos a necessidade de que houvesse aqui no País também alguma forma de regulamentação. Nós, da área jurídica, conhecíamos pouco sobre o assunto; tivemos que estudar, porque não conhecíamos, naturalmente, a legislação, a prática e os mecanismos de funcionamento da certificação digital. Tivemos que nos informar, estudar muito, contando com a ajuda de especialistas. O professor Miguel

Teixeira Carvalho, do Ministério da Ciência e Tecnologia na época, e o pessoal do Serpro nos ajudaram muito no entendimento da certificação digital e os conceitos de chave pública, chave privada, algoritmo de hash e outros. E, ao entender a certificação digital, tivemos também que entrar no conceito de Autoridade Certificadora e Autoridade Raiz, o que foi muito importante para depois estabelecer o modelo.”

**Fonte: O senhor participou ativamente da concepção da ICP-Brasil, ajudando a definir o modelo de certificação que foi adotado no País. Como foi feita essa escolha?**

“O modelo de certificação digital que o Brasil adotou está na Medida Provisória 2200. Foram estudados os modelos do mundo e o Governo optou por adotar o modelo vigente na Comunidade Européia, previsto na Diretiva 93/1999, por dois motivos: primeiro, devido à similitude da legislação – a nossa legislação é uma herança do sistema romano-germânico, nossas leis são baseadas nas leis portuguesas, espanholas, italianas, e sofrem muita influência do direito alemão. A maneira de legislar brasileira, a nossa maneira de agir no processo judicial, é muito mais próxima do sistema europeu. Chegamos à conclusão de que seria, portanto, mais fácil para o mundo jurídico brasileiro assimilar, com mais rapidez, um conjunto de normas que tivesse uma sistemática européia do que uma sistemática americana.

O segundo motivo é que a sistemática européia é compatível com a sistemática americana, mas o contrário não ocorre. Se



adotássemos o modelo europeu, o sistema brasileiro conversaria com os americanos; mas se adotássemos o modelo americano, teríamos dificuldades para conversar com os europeus. É que a Diretiva Européia 93/1999 dá padrões mínimos básicos de organização do sistema, mas, ao mesmo tempo, ela tem que ser flexível o suficiente para respeitar as diversidades culturais de cada país. A Diretiva, portanto, não poderia ser muito rígida.

Resumindo, as coisas funcionam mais ou menos assim: na medida em que nós respeitamos a Diretiva Européia, passamos a ser como “um membro da comunidade européia”. Se os sistemas dos vários países falam entre si, falam também com o nosso. Isso, para negociações futuras, facilita nosso ingresso na Europa; e o sistema americano é absolutamente aberto, na realidade, aceita qualquer um.”

### **Fonte: O que exatamente determina a Medida Provisória 2200?**

“A opção do Governo está sintetizada na MP-2200, que prevê dois sistemas paralelos, que operam simultânea e livremente: um sistema de certificação livre e um sistema de certificação governamental.

Para este, foi criada a Autoridade Raiz única – que é o ITI –, uma autarquia federal, a Infra-Estrutura de Chaves Públicas hierarquizada, dentro da estrutura da ICP. A MP estabeleceu ainda que a Autoridade Raiz não tem contato com o usuário, quer dizer, ela não é a fornecedora do certificado no nível do usuário; ela certifica as autoridades certificadoras de segundo nível, que

podem ser órgãos públicos ou privados. Ou seja: a MP criou o modelo da infra-estrutura e fixou as atribuições legais do sistema público e privado, copiando rigorosamente a Diretiva Européia.”

### **Fonte: Faça, por favor, um paralelo entre uma operação apoiada pela ICP-Brasil e uma feita fora dessas regras.**

“Em pouquíssimos casos, há a obrigatoriedade de se trabalhar com a autoridade pública. Na prática, é o seguinte: se você trabalha com a ICP-Brasil e assina um documento eletrônico, você não pode negar que assinou o documento. E a parte do outro lado tem o direito de presumir que você o assinou. Se você quiser dizer que aquele documento não foi assinado por você, você tem que fazer a prova. É a presunção de autoria. É uma operação mais segura, porque equivale a uma operação com testemunhas. A Autoridade Raiz e a Autoridade Certificadora são testemunhas de que você é você – o Governo certifica que você é você e a Lei presume que você é o autor do documento.

Fora da ICP, acontece o contrário: se a outra parte duvidar da autoria, cabe ao emitente provar a autenticidade de sua assinatura. As operações são mais tranquilas e mais rápidas porque a outra parte aceitará a sua assinatura se quiser; se não quiser, ela não concorda que você assinou e não faz a operação. E se ela questionar a sua assinatura, você é que tem que provar que ela é autêntica.

Fora da ICP, você não terá uma autoridade: você terá uma

testemunha privada que as partes aceitarão se e na medida em que quiserem. Por exemplo, duas empresas podem contratar uma certificadora privada e fazer negócios, sem problema nenhum, fora da PKI ou ICP oficial.”

### **Fonte: Na prática, como o mercado assimilará esses dois sistemas paralelos?**

“Eu acredito que será o seguinte: na maioria das operações comerciais de baixo valor, você não usará certificação nenhuma, permanecerá como está funcionando atualmente, com cartões de crédito, por e-mail por exemplo. Eu não vou querer comprar um cartão de certificação para isso. E o entregador de gás ou pizza também vai continuar da mesma forma. A certificação seria um custo a mais.

Para as operações de porte médio, eventualmente as empresas vão contratar infraestrutura particular. Não será necessário entrar na esfera governamental, que é mais cara porque a segurança é maior. Se você não precisa de muita segurança, não há motivo para aumentar o custo.

Agora, para documentos oficiais, para os quais a Lei exige autenticidade, aí, nesses poucos casos, você será obrigado a entrar no sistema da ICP-Brasil; ou ainda se o valor das operações for muito alto ou se, por segurança, as partes optarem também pela ICP-Brasil. E as empresas certificadoras também têm inteira liberdade. A mesma empresa pode oferecer serviços dentro da ICP e fora da ICP.

O que vai acontecer é que a certificação emitida pela ICP-

Brasil vai custar mais caro; fora do sistema, a empresa não vai precisar pagar taxas por esse documento, não é submetida à fiscalização e não é exigido dela um certo padrão de qualidade, como a ICP-Brasil, que tem padrão internacional. A nossa Autoridade Raiz – que é o ITI – tem que estar e está no mesmo padrão de qualidade da Europa.”

**Fonte: Comente a certificação digital como solução para a questão da segurança. Como esse expediente se contrapõe ao uso do documento em papel?**

“No fundo, nós convivemos com o uso da correspondência eletrônica em grande escala: hoje, você troca muito e-mail, muita correspondência por computador. Além do e-mail, há também o sistema de mensagem direta, que são os messengers, e o sistema de imagem também – brevemente a certificação vai ter que contemplar a imagem. Daqui a pouco, você vai ter a conversa na internet com som e imagem, gravá-los em CD e com possibilidade de certificação do CD.

A partir de um determinado momento, a comunicação pela internet perde a confiabilidade. Isso acontece mais ou menos como com o telefone e com o fax. Ninguém compra, por exemplo, uma casa por telefone. Tanto vendedor quanto comprador vão querer tudo bem escrito, documentado, com testemunhas, em cartório. Há o serviço de telepizza – por telefone –, mas não há o telecasa. Há vários serviços de comércio por telefone. Mas algumas operações, a partir de um certo valor, você não vai fazer por telefone. Você vai querer se certificar da operação.

Em geral, a certificação se faz em papel: você faz um contrato, busca testemunhas, registra em cartório. Na verdade, a certificação digital não se dirige para a grande massa de operações comerciais. É um engano achar isso. Funciona da mesma forma que a certificação em papel, que você faz para operações de grandes valores, duradouras. Assim como você não faz a compra de uma casa ou apartamento, por telefone, você também não faz uma escritura pública para comprar um sanduíche. Ali é importante justamente que não tenha a certificação. Porque ela torna o

**“Na verdade, a certificação digital não se dirige para a grande massa de operações comerciais. É um engano achar isso.”**

processo mais lento e, nos negócios de grande escala, de pequeno valor unitário, você quer velocidade, e a certificação vai atrapalhar isso. A relação custo-benefício faz valer a pena o risco.

Para ilustrar: quando você pede uma entrega de gás, por telefone, você pode estar falando com o Jack, o Estripador. Há uma possibilidade mínima de não ser o entregador de gás. Da mesma forma que o rapaz do gás pode estar recebendo o telefonema do Jack, o Estripador. Se, toda vez que se fizer uma operação dessa natureza, for exigido documento de identidade, ou outros, ele não vai vender nenhum botijão de gás.

Ele, portanto, tem que correr algum risco.

Isso vale, da mesma forma, para a compra de uma passagem aérea pela internet: você quer facilidade, velocidade, portanto, não se usa a certificação. E tem funcionado. A empresa aérea que exigir que o cliente tenha um cartão, um token ou um outro elemento de certificação está criando um complicador para o cliente. E o que ela quer é facilitar. Isso já vale até para os cartões de crédito. Já se dispensa, em muitos casos, a assinatura do titular, bastando informar o número do cartão. O cartão já dispensou a certificação – que é a nossa assinatura – para ganhar tempo.”

**Fonte: Em que casos, então, a certificação é a solução mais indicada?**

“Ela entra quando você quer ter perenidade e durabilidade na informação, para que outros possam saber que a operação foi feita. A operação ou o documento será armazenado por longo tempo, como alguns documentos públicos ou por exigência legal. Ou quando o valor da operação é tão grande que você deseja uma segurança a mais.

Enfim, a certificação não é nada mais nada menos que um processo de autenticação, não do documento, mas da autoria do documento. Em algumas operações, você tem que saber com certeza com quem está falando, quem está enviando a mensagem. Em outras, você não precisa ter certeza; você presume a certeza. A quantidade de ligações telefônicas que fazemos, e-mails e fax que transmitimos mostra que a maioria das mensagens que

trocamos dispensa um tipo de certificação mais séria. Em geral, você se contenta com o nome da pessoa no cabeçalho do e-mail, o que é facilmente falsificável.

A estrutura da ICP-Brasil funciona para uns poucos casos em que é obrigatória. Fazendo um paralelo: quando é que nós somos obrigados a ir a um cartório passar uma escritura? Em pouquíssimos casos.

Na maioria das vezes, nós fazemos os nossos negócios por documentos particulares. A ICP, da mesma forma, é obrigatória em um número limitadíssimo de casos e ela faz uma remissão para o Código Civil Brasileiro. Na maioria dos casos, a ICP não é obrigatória: você pode trabalhar com ICPs particulares, privadas e fora do sistema governamental.”

**Fonte: Com relação ao comércio eletrônico, há uma grande expectativa de aquecimento nesse tipo de transação. Essa expectativa é procedente?**

“Fala-se muito em comércio eletrônico. É um engano pensar que a certificação digital é importante para o comércio eletrônico. Na verdade, o comércio eletrônico em geral não vai usar a certificação, ou vai usar muito pouco. Na minha opinião, é muito importante para a maioria das transações comerciais justamente que não haja o processo de certificação, a fim de agilizar esse tipo de operação.”

**Fonte: Na prática, como funciona no setor público o uso da certificação digital?**

“No Governo Federal, desde 2000, as correspondências

oficiais dos ministros ao Presidente da República – propondo projetos de lei, projetos de decretos, minutas de medidas provisórias – são feitas, transmitidas e assinadas eletronicamente. Cada ministro de Estado tem seu cartão, sua senha, e os documentos são transmitidos para a Casa Civil com a garantia de autenticidade não do transmissor da mensagem, mas do autor do documento.

A certificação digital substitui a assinatura em papel. E quem recebe o documento tem a mais absoluta certeza de que foi produzido por determinado ministro, por determinada autoridade. Não se faz mais esses documentos em papel.

A Casa Civil, inclusive, recusa quando feitos em papel. Era assim nos dois últimos anos do governo Fernando Henrique, mas acho que não mudou a sistemática. Cada ministro de Estado, cada secretário de Ministério tem a sua senha, que é o seu cartão magnético, é um cartão com um chip contendo exatamente a chave privada com um algoritmo.”

**Fonte: Como será a aplicação da certificação digital em Minas?**

Será a mesma coisa: temos aqui a Advocacia Geral, a transmissão de documentos oficiais para o Palácio, a transmissão de documentos do Palácio para a Imprensa Oficial. Hoje é necessário adotar as duas formas: envia-se o documento por meio eletrônico, mas, por segurança, o papel vai atrás. Quando tivermos a certificação digital, vamos acabar com o papel. Vamos ganhar tempo.”

**Fonte: Sintetize, por favor, os benefícios da certificação digital para a administração pública.**

“Você ganha velocidade na transmissão da informação eletrônica; já tem isso, mas você passa a transmitir dados e documentos por meio eletrônico que você não poderia fazer se não estivesse na ICP-Brasil.

Não se pode, hoje, mandar um documento oficial para o governador e não assinar; eu tenho que assinar, qualquer secretário que mandar um documento oficial tem que assinar.

Não se pode, hoje, mandar um documento oficial para o governador por e-mail, ainda que o governador se disponha a receber esse e-mail.

Primeiro, o governador tem um problema de segurança: ele não sabe se quem está passando aquele e-mail é o próprio secretário ou um auxiliar dele; segundo, ele não tem certeza quanto à autenticidade do documento: ele não sabe se o documento foi modificado no meio do caminho ou se o documento não foi modificado no seu próprio computador. Com a certificação, se ele estiver assinado e alguém fizer alguma alteração, essa assinatura cai; saberemos que esse documento sofreu uma alteração.

Ganhamos na velocidade e eliminamos o office-boy em muitas circunstâncias. Ganhamos na velocidade, no tempo, na distância.”

**Fonte: Quais são as vantagens de uma entidade pública no processo de**



## **certificação digital?**

“Com a certificadora pública, você passa a ter um pouco mais de liberdade. No caso da Prodemge, por exemplo, como uma Autoridade Certificadora dentro da ICP-Brasil, passamos a ter a liberdade de, nós mesmos, emitirmos os nossos certificados, tendo as nossas autoridades de registro. Mas, provavelmente, a Prodemge não vai entrar no mercado privado para competir com empresas privadas de certificação, mesmo porque o perfil dela é voltado para servir ao Estado.

Isso equivale mais ou menos também àquela história: o Estado pode ter ou não a sua própria companhia de energia elétrica; Minas tem a Cemig. Não sei se outros estados têm, mas nem por isso o pessoal de lá está no escuro. É claro que você, tendo o serviço próprio, passa a ter uma certa liberdade. Não é bom nem ruim, depende da conveniência.”

**Fonte: Como o senhor avalia a questão da tradição do uso do documento em papel, que é algo palpável, com a entrada do documento digital, através da certificação?**

“O papel não vai acabar. Na medida em que você certifica um documento eletrônico, você passa a poder armazená-lo com segurança. Não com segurança da duração do armazenamento, mas com segurança da autenticidade do documento. Uma coisa é você achar um papel velho; outra é você achar um papel velho com uns rabiscos e uma assinatura do Beethoven embaixo. Ah, isso aqui é o original da Quinta Sinfonia!

Na medida em que o papel passou a ser assinado, ficou importante ele ser guardado. Da mesma forma, na medida em que o documento eletrônico possa ser assinado, pode-se armazenar esse documento, ele começa a ficar importante, porque ele passa a ter o valor do papel assinado. Recentemente, entreguei ao Arquivo Público Mineiro algumas dezenas de metros de papéis que eram originais de decretos desde mais ou menos 1940 até hoje. Eram os originais, que estavam guardados aqui porque são produzidos aqui. Se, mais tarde, o governador estiver fazendo assinaturas eletrônicas de decretos, eu não vou ter decretos aqui,

**“Os documentos do Qumran duraram 2 mil; estão arquivados há 2 mil anos. Não sabemos se daqui a 500 anos alguém vai ler um disquete.”**

arquivados em papel, mas arquivados eletronicamente. Ao invés de metros de papel, eu vou ter alguns centímetros de CDs numa caixinha, que eu posso, inclusive, duplicar e enviar para o arquivo até pela internet.”

**Fonte: Com relação à mídia de armazenamento dessas informações e documentos, o senhor se preocupa com os meios de recuperação das informações. Comente esse aspecto.**

“Temos que considerar as

mesmas dificuldades de um microfilme, por exemplo. Eu tenho em minha casa algumas dezenas de LPs antigos e tenho lá um toca-discos que está sem agulha. Eu estou atrás de uma agulha para esse toca-discos. Todos já estão duplicados em CD, mas eu gosto do LP. Ou seja, a minha mídia está ficando ultrapassada. Quem guardou alguma coisa naqueles disquetes de 5 ¼ e não passou para outra mídia perdeu informação. Vai ter que ir a um museu para recuperá-los – você vai ter que trabalhar com a arqueologia eletrônica. Há essas susceptibilidades. Não vamos pensar que o meio eletrônico é a grande solução. Ele tem problemas. Obviamente, na sepultura dos nossos parentes, nos cemitérios, nós vamos continuar colocando o nome na pedra, no mármore, porque nós queremos que isso dure muito. Ninguém vai largar um chip na sepultura.

A pedra é uma das mídias mais duráveis que já se descobriu. O homem da pedra descobriu, quando começou a escrever, que tratava-se de uma mídia durável. Não era só porque não tinha o papel. Não é prático, mas tem muita escrita em pedra que recuperou a nossa história. Nós não sabemos a durabilidade de um CD. A carta de Pero Vaz de Caminha já durou 500 anos; nós não sabemos se a mídia eletrônica se conserva por 500 anos. Os documentos do Qumran duraram 2 mil; estão arquivados há 2 mil anos. Não sabemos se daqui a 500 anos alguém vai ler um disquete.

A certificação permite que você passe a ter um armazenamento importante de informações, mas, eventualmente, como não é um armazenamento físico, você tem

um problema de recuperação. É mais fácil recuperar informação de um LP do que de um DVD ou de um disquete de computador, em que o armazenamento é lógico.

A certificação digital valoriza muito o armazenamento da informação eletrônica, porque ele passa a ser um armazenamento com alto grau de confiabilidade quanto à autenticidade. Ela agrega valor ao documento. Mas a certificação não acrescenta nada com relação à durabilidade. Mesmo a certificação privada, é importante, por exemplo, para documentos históricos particulares. A carta de Pero Vaz de Caminha é um documento oficial, tratava-se de um escrivão do rei na esquadra, uma autoridade pública.

De outra forma, são documentos particulares os Lusíadas, Odisseia, a Ilíada. Mesmo a certificação privada agregará valor a documentos privados arquivados com certificação digital privada.”

**Fonte: *Sistemas da Microsoft estariam adaptados para o sistema brasileiro de certificação digital. Como funciona?***


“No caso da chave pública brasileira, foi assinado, em 2002, um convênio entre o Governo brasileiro e a Microsoft. A partir daquela data, a chave pública brasileira estaria fazendo parte do sistema da Microsoft. Nós somos um dos poucos países do mundo a fazer esse acordo com a Microsoft. Como funciona: para usar o sistema de certificação, no seu computador, há o sistema de senha e contrasenha e o seu computador tem que conhecer a contrasenha da autoridade

certificadora da autoridade raiz, ou seja, essa contrasenha tem que estar nos sistemas, é a chave pública.

Se ela não estiver nos sistemas, você vai ter que baixá-la no computador. Se você vai trabalhar com a ICP, vai ter que entrar no site da autoridade raiz, baixar a chave pública no seu computador, armazenado-a na memória. Na hora em que você fizer comunicações usando assinaturas eletrônicas, o computador da outra parte, ao receber a sua mensagem, vai ter condições de lhe dizer que a autoridade raiz está garantindo a operação. Se isso não está no computador, você tem que fazer algumas operações manuais para consultar a raiz ou consultar a certificadora.

É mais ou menos isso: alguém me telefona e diz uma senha; você tem que dar a contrasenha. Aí você teria que ligar para uma terceira pessoa e confirmar se senha e contrasenha estão compatíveis, porque você não confia na ligação, mas você confia em quem vai lhe dar informações sobre a senha, que é a autoridade certificadora. Esse sistema pode ser on-line ou através de vários passos. Uma vez dentro do sistema da Microsoft, é como se houvesse uma linha com a raiz.

A Microsoft permite que, na hora que você colocar o sistema de senha e contrasenha ou de chave pública e chave privada no computador, a consulta seja feita automaticamente. E, no computador, você já pode saber se o documento é válido. Com esse acordo, isso já vem no sistema. A Microsoft só fez isso depois de ter uma declaração formal do Brasil de que a nossa Autoridade Raiz atende a uma série de requisitos

que ela solicitou. Eles quiseram auditar o sistema, mas isso nós não permitimos.” 



# ICP-Brasil

## Evolução com Equilíbrio e Correção

Evandro Oliveira

Após um tempo considerável, desde que a certificação digital no Brasil tomou rumos mais claros e específicos (a Medida Provisória 2.200-2 sobre o tema foi publicada em agosto de 2002), ainda encontramos pessoas que, mesmo atuando na área de informática, mesmo sendo profissionais qualificados, ainda não conhecem o funcionamento, aplicabilidade e exemplos práticos das vantagens de se ter a adoção de uma Infra-estrutura de Chaves Públicas (de PKI - Public Key Infrastructure).

Alguns casos de não reconhecimento chegam a repetir certa técnica muito utilizada noutro tema muito polemizado ultimamente, o software livre. Os desconhecidos utilizam da aplicação do medo, da incerteza e da dúvida (FUD, da expressão em inglês) quanto à eficácia e correção do processo de Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), com argumentos que são do domínio de parcela que nem mesmo discute o tema com qualidade.

Embora a ICP-Brasil preveja que particulares possam utilizar qualquer tipo de certificação, ainda são muitos os profissionais de informática que não entenderam em quais condições devem usar processos diferenciados de certificação digital. Entendemos que se os profissionais de TI passarem a usar certificados digitais, assinaturas eletrônicas, criptografia assimétrica e até mesmo criptografia

simétrica, com a preocupação de interoperabilidade entre estes mecanismos, constatarão que a estrutura adotada no Brasil é a mais apropriada aos propósitos de Governo e Setor Privado.

Mas como é natural que mais pessoas passem a questionar os processos existentes e vejam as vantagens do uso de certificação digital como um grande passo na melhoria e segurança dos

procedimentos e transações feitas por particulares e por estes e o poder público, o que estamos presenciando é uma crescente adoção e aceitação dos regulamentos previstos na MP 2.200-2 e nas resoluções publicadas pelo Comitê Gestor da ICP-Brasil.

Para começar a entender o funcionamento dessa estrutura, é necessário saber a diferença entre as formas e processos de certificação digital e a hierarquia adotada no País ([www.iti.gov.br](http://www.iti.gov.br)). O regulamento implantado determina que as regras devem

ser aprovadas pelo Comitê Gestor que tem representação do Poder Executivo Federal e da Sociedade Civil (com previsão de que os Poderes Legislativo e Judiciário passem a ter representação no referido Comitê). Este Comitê é assessorado por um Conselho Técnico que estuda e debate as questões técnicas, questões jurídicas e administrativas e adoção de tecnologias para promover a interoperabilidade entre certificados de autoridades certificadoras diferentes da estrutura.

**“Os desconhecidos utilizam da aplicação do medo, da incerteza e da dúvida quanto à eficácia e correção do processo de Infra-estrutura de Chaves Públicas Brasileira...”**

A Autoridade Certificadora Raiz, representada pelo Instituto Nacional de Tecnologia da Informação – ITI ([www.iti.br](http://www.iti.br)) –, autarquia vinculada à Casa Civil da Presidência da República, cuida para que a operação das autoridades certificadoras, autoridades de registro, prestadores de serviço, auditorias independentes e demais intervenientes possam atuar na estrutura com as melhores condições e funcionalidades.

As empresas da iniciativa privada e órgãos públicos já estão se posicionando de forma a escolher onde estão mais aptos e adequados a atuar com certificação digital na estrutura da ICP-Brasil e, após serem auditados para mostrar conformidade com as regras estabelecidas, recebem o credenciamento e podem atuar com os demais e servindo ao cidadão com garantias que não presenciemos em métodos de certificação não auditáveis. Cabe então a cada um desses intervenientes estudar o tema, se apresentar como capaz para desempenhar o papel que deseja e, após credenciado, se qualificar como debatedor e participe da evolução do processo.

Confiar que a estrutura estabelecida pode determinar as técnicas e tecnologias a serem adotadas e que as auditorias são realizadas com intuito de verificar o proposto e realizado pelas entidades credenciadas é mais importante do que não participar e querer que um ponto aqui e outro acolá seja modificado para atender interesses corporativos e particulares.

As regras de ICP-Brasil têm evoluído a partir da primeira estrutura montada, e devemos ressaltar

que é importantíssimo não “jogar fora” o investimento valioso já implementado e em uso no País. Não se deve nem imaginar o estrago que poderia ser feito se o Sistema de Pagamentos Brasileiro, o maior exemplo do uso prático da certificação digital no País, tivesse que ser refeito. Outro exemplo a ser referenciado daqui a alguns dias é o uso integral, por parte dos servidores da Receita Federal, de certificados digitais da ICP-Brasil.

Trabalhamos para, a cada reunião do Comitê Gestor, propor revisões que consolidem, cada vez mais, a inserção de instituições do setor público que não sejam da esfera federal, não pelo método do medo, incerteza e dúvida, mas por contribuirmos para que todos acreditem que estão fazendo a escolha por sistemas criptográficos apropriados e, a partir daí, passem a contribuir com o País na adoção e aplicação das estruturas e regras da ICP-Brasil, elevando consideravelmente os níveis de segurança nas transações que utilizem as mais variadas tecnologias da informação.

**“As empresas privadas e órgãos públicos já estão se posicionando de forma a escolher onde estão mais aptos e adequados a atuar com certificação digital...”**

**Evandro Oliveira**

**Diretor de Auditoria, Fiscalização e Normalização  
Instituto Nacional de Tecnologia da Informação –  
ITI – Casa Civil – Presidência da República**



# Governo Eletrônico Seguro

## O projeto de segurança da informação do governo mineiro

Renata Vilhena

Com o crescente uso das novas tecnologias da informação e comunicação, principalmente com o advento da internet, e com a importância da informação enquanto recurso estratégico, a segurança da informação passou a ser uma das principais preocupações das organizações, sejam elas públicas ou privadas.

No que tange às organizações públicas, inserem-se, num contexto de modernização do Estado, propostas que envolvem novas tecnologias da informação e comunicação nas relações entre Governo e Cidadão (G2C), Governo e Empresas (G2B), Governo e Servidores (G2E) e Governo e Governo (G2G). Entretanto, nessas relações, é necessário um aparato que dê garantias e confiabilidade nas transações eletrônicas entre o Governo e a Sociedade.

Nesse sentido, o Governo do Estado de Minas Gerais, em consonância com o Programa de Governança Eletrônica, está promovendo ações com o intuito de desenvolver um projeto de implantação de Modelo de Gestão de Segurança da Informação na Administração Pública do Poder Executivo Estadual.

Sob coordenação da Secretaria de Estado de Planejamento e Gestão (Seplag) e em parceria com a Secretaria de Estado de Fazenda (SEF) e da Companhia de Tecnologia da Informação de Minas Gerais (Prodemge), o Projeto de Segurança da Informação tem como objetivo preparar as referidas instituições para alcançar um nível de segurança desejada.

Para tanto, serão realizadas atividades que vão desde uma ampla análise de riscos em seus ativos tecnológicos e seus principais processos de negócio

até a elaboração e divulgação de política de segurança da informação, capacitação de técnicos e campanhas de sensibilização de usuários, desenvolvimento de um Plano Diretor de Segurança da Informação e de um Plano de Continuidade de Negócios.

Outra ação de destaque diz respeito à capacitação tecnológica da Prodemge, que se tornará um Security Provider, contando com a parceria da Módulo, empresa brasileira com maior renome em segurança

da informação no País, com mais de 19 anos de existência e considerada uma das maiores empresas de segurança da informação do mundo. Pretende-se também obter a Certificação Internacional da Prodemge junto à BS 7799, norma de referência internacional em segurança da informação.

Enfim, esse projeto, em consonância com a Certificação Digital - projeto em andamento e coordenado pela Prodemge - proporcionará ao Governo do Estado infra-estrutura de tecnologia da informação e comunicação e processos de negócios seguros. Dessa forma, a Administração Pública do Poder

Executivo Estadual estará apta para a prestação de informações e serviços eletrônicos de forma segura, fortalecendo os mecanismos de participação dos cidadãos e transformando as relações entre Estado e Sociedade, condição fundamental para a inserção efetiva do Estado de Minas Gerais na sociedade da informação.

**“...o Governo de Minas, em consonância com o Programa de Governança Eletrônica, está promovendo ações para desenvolver um projeto de implantação de Modelo de Gestão de Segurança da Informação na Administração Pública do Poder Executivo Estadual.”**

**Renata Vilhena**

**Secretária-adjunta de Planejamento e Gestão do Governo do Estado de Minas Gerais**





# Criptografia na ficção

## Técnicas antigas e fantasias modernas

Luís Carlos Silva Eiras

A mais famosa mensagem secreta da ficção foi escrita na parede do palácio do rei Baltazar: “*Menê menê tequêl u-parsîn*”. E foi decifrada pelo profeta (e criptólogo) Daniel, conforme se lê no capítulo 5 do seu livro, e é sobre o breve futuro do rei – Baltazar morreu momentos depois da mensagem lida. Da Bíblia para cá, muitos são os exemplos de mensagens secretas em narrativas, já que boa parte da ficção conta a história de investigações e, com uma mensagem a ser decifrada, já se tem o principal da história.

É o que faz Edgar Allan Poe em *O Escaravelho de Ouro*, novela publicada em 1843. Conta como um pergaminho, descoberto numa praia, continha uma mensagem secreta e como ela foi decifrada, possibilitando que se achasse um tesouro de piratas. Allan Poe se concentra primeiro em explicar que, a partir de uma tabela de frequência, os caracteres sem sentido vão, aos poucos, revelando um texto – que, por sua vez, não faz o menor sentido! Então, Poe usa a imaginação para revelar o sentido desse texto e achar o tesouro. Uma proeza de dupla decifração.

Não era a primeira vez que Poe tocava no assunto. Em 1841, publicou num jornal que tinha recebido duas mensagens secretas de um certo W. B. Tyler, mas, apesar de ter decifrado mais de cem mensagens, estava sem tempo (!) para resolvê-las, deixando isso para os leitores. Essas mensagens

demoraram 150 anos para ser decifradas, a primeira, em 1992, por Terence Whalen, e, a segunda, em 2000, por Gil Broza, o que acabou com qualquer dúvida sobre quem era o tal W. B. Tyler. Allan Poe escreveu ainda o ensaio *Criptografia* (1842), uma prévia de *O Escaravelho de Ouro*.



Outro autor famoso que usa o assunto é Júlio Verne. Em *Matias Sandorf* (1885), a criptografia é feita através de uma tabela de três colunas de letra, sobre a qual se colocam cartões perfurados. As letras que ficam visíveis formam a mensagem. Com esse método, foi possível decifrar neste ano o manuscrito Voynich, 230 páginas de uma escrita incompreensível por mais de 5 séculos. Agora se sabe: o manuscrito não faz mesmo sentido e trata-se de uma fraude.

Mesmo em romances mais recentes, são utilizadas criptografias antigas como no *O Nome da Rosa* (1980) e *O Pêndulo de Foucault* (1988), de Umberto Eco. O primeiro usa a substituição de palavras por símbolos, o segundo, o cifrário de Vigenère, conhecido desde o século XVI.

Carl Sagan, em *Contato* (1985), é que inventa algo complicado. Imagens da transmissão de TV das

Olimpíadas de Berlim, de 1936, foram capturadas por extraterrestres e reenviadas para a Terra. Só que, no meio das frequências da velha transmissão, havia mensagens para os terráqueos. Michael Crichton, em *Esfera* (1987), é mais modesto. Uma nave espacial encontrada no fundo do Oceano Pacífico envia uma seqüência de números, que vão aos poucos sendo reagrupados até formarem mensagens inteligíveis.

Mais recente, *Cryptonomicon*, de Neal Stephenson, de 1999, faz a ligação entre os decifradores dos códigos alemães da Segunda Guerra Mundial e os hackers atuais, para quem conseguir atravessar as suas 900 páginas de idas e vindas no tempo.

No cinema, também aparecem criptografias bem variadas, que tentam, às vezes, se aproximar da realidade. Não é o caso de *Quebra de Sigilo* (1992), onde Robert Redford vai atrás de uma caixa capaz de quebrar a senha de qualquer computador, já que a caixa sabe como funcionam os números primos<sup>1</sup>. Nem de *Código para o Inferno* (1998), onde Bruce Willis se envolve com um garoto autista que sabe ler códigos secretos, que custaram um bilhão de dólares para ser desenvolvidos. Muito menos é o caso de *A Senha* (2001), onde um hacker consegue digitar mais rápido do que um programa de segurança.

Mas é o caso de *Enigma* (2001). Dougray Scott faz um matemático mais ou menos baseado em Alan Turing e mostra como os ingleses decifraram os códigos secretos dos alemães utilizando o *Colossus*, o primeiro computador. (Mostra também, numa cena de bar, Mick Jagger, o produtor do filme.) Turing é o personagem principal da peça *Breaking The Code* (1987), de Hugh Whitmore, onde conta como ele e Churchill leram todas as mensagens secretas dos

nazistas, inclusive a localização do *Bismarck*, o que possibilitou seu afundamento em 1941<sup>2</sup>.

Já o filme *U-571* exagera na importância da captura de uma máquina Enigma num submarino alemão pelos americanos. Os poloneses conheciam o funcionamento da máquina desde o início dos anos 30 e repassaram esse conhecimento para os franceses e ingleses. Eles sabiam também que não era suficiente conhecer seu funcionamento para decifrar as mensagens codificadas. Porém, a versão

em DVD tem uma boa entrevista com David Kahn, autor do clássico *The Codebreakers* (1996), ainda não editado no Brasil.

Mas é em *Uma Mente Brilhante* (2001) que essa história de decifrar códigos secretos aparece em filme da maneira mais interessante. Russel Crowe faz o matemático John Nash, que era capaz de ler códigos secretos russos escondidos em notícias de jornais e revistas. Todos imaginários.

“... boa parte da ficção conta a história de investigações e, com uma mensagem a ser decifrada, já se tem o principal da história.”

## NOTAS

<sup>1</sup> Se você também sabe como funcionam os números primos, você pode ganhar um milhão de dólares. É só responder sobre a conjectura de Riemann para o Instituto Clay de Matemática do MIT. Mais informações em <http://www.claymath.org/millennium/>.

<sup>2</sup> O funcionamento do Enigma, do Colossus e de outros métodos citados aqui pode ser testado pelo leitor em <http://www.apprendre-en-ligne.net/crypto/>.

**Luís Carlos Silva Eiras**

Analista de Sistemas da Prodemge

# Certificação Digital:

## o fio de bigode eletrônico

**Confiança e segurança. As bases históricas das relações, sejam elas comerciais ou não, sobrevivem intactas, ao longo do tempo, às mudanças culturais, sociais ou tecnológicas, embora agora marcadas pela impessoalidade. São fundamentos de grandes e pequenas operações, condições para que alianças se concretizem.**

**O velho "fio de bigode", a caderneta do armazém ou a palavra empenhada, atributos incontesteáveis de confiança, que vêm assegurando a confiabilidade das partes envolvidas em qualquer transação comercial, ganham, como tudo na era digital, a sua versão eletrônica.**

**Adaptado à consolidação da internet e ao crescimento desenfreado das operações feitas através da rede mundial de computadores, um novo recurso tecnológico passa a se integrar aos poucos à vida dos brasileiros: a certificação digital, que agrega aos documentos eletrônicos, inclusive aos e-mails, a garantia de sua autoria e autenticidade, imprimindo às operações eletrônicas segurança e confiabilidade.**



instantaneidade que a tecnologia imprime às comunicações passou a exigir mecanismos que assegurem às empresas, sejam elas públicas ou privadas, e às pessoas, físicas ou jurídicas, pleno aproveitamento do potencial oferecido pela tecnologia da informação.

A certificação digital é um arquivo eletrônico que acompanha um documento assinado digitalmente, contendo informações que identificam a empresa ou a pessoa com quem se está tratando na rede. Um documento eletrônico com certificação digital tem, portanto, validade jurídica. Isso garante sua autenticidade de origem e autoria, integridade de conteúdo, confidencialidade e irretratabilidade, ou seja, que a transação, depois de efetuada, não possa ser negada por nenhuma das partes.

Além da segurança e velocidade na tramitação de documentos, a certificação digital transcende a questão de espaço, ao permitir, por exemplo, que um executivo possa assinar normalmente um documento juridicamente válido a partir de qualquer ponto geográfico e em qualquer horário, com o mesmo valor de um documento em papel. Viabiliza ainda a guarda e o arquivamento seguros de documentos - oficiais ou não - com a mesma validade do seu original em papel.

O diretor de Infra-Estrutura de Chaves Públicas do ITI - Instituto Nacional de Tecnologia da Informação - autarquia federal vinculada à Secretaria da Casa Civil da Presidência da República, Renato Martini, resume os benefícios do uso dessa tecnologia. Para ele, a certificação digital agrega aos serviços maior segurança, transparência, desmaterialização, redução do consumo e trânsito de papéis, contribuindo para a diminuição do custo Brasil. Do ponto de vista institucional e social, melhora a relação do Governo com o cidadão e abre possibilidades para oferta de mais serviços pela internet - o cidadão não precisa sair de casa para ter acesso a uma série de serviços, na medida em que esteja equipado para se identificar na rede.

A assinatura eletrônica não é, no entanto, a digitalização de uma assinatura, mas um complexo sistema de códigos. Para o advogado especialista em Direito Internacional e professor gaúcho Fabiano Menke, ex-procurador



geral do Instituto Nacional de Tecnologia da Informação, a assinatura digital é um meio de agregar confiança ao ambiente virtual, confirmando a importância da autoria e identificação principalmente para questões legais. A assinatura digital agrega à internet, segundo ele, o atributo da identificação: tem, portanto, os mesmos efeitos de uma assinatura manuscrita feita no papel.

Um certificado digital contém informações relativas a seu usuário: a codificação de sua assinatura (chave privada), nome e endereço de e-mail, identificação da Autoridade Certificadora, número de série, a assinatura digital e o período de validade do certificado, que pode ser de um ou dois anos.

A chave privada do usuário pode ser armazenada em seu microcomputador, ou ainda num smart card ou token, que são mídias portáteis, que permitem seu uso a partir de outras estações. O acesso às informações contidas em seus chips é feito por meio de uma senha pessoal, determinada pelo titular. O smart card assemelha-se a um cartão magnético, sendo necessário um aparelho leitor para seu funcionamento. Já o token assemelha-se a uma chave e requer a conexão à porta USB do computador. A segurança desses três recursos é garantida também por senha.

Quanto aos preços, podem ainda ser considerados altos. Segundo o presidente da CertiSign, uma das empresas certificadoras credenciadas pela ICP/Brasil – Infra-Estrutura de Chaves Públicas, Sérgio Kulikovsky, “a média é de R\$100,00 por certificado (com validade de um ano), considerado compatível com a capacidade do usuário”. Ele prevê que esse preço caia a médio prazo: “Naturalmente, na medida em que se aumenta a demanda, o preço cai, uma vez que é estabelecido em função da quantidade”. E conclui: “Se o serviço oferecido é bom, o preço se justifica pelo benefício que ele oferece”.

### **Chaves Públicas - a questão legal**

No Brasil, a exemplo do modelo adotado pela comunidade européia, a certificação digital pode ser

concedida a pessoas físicas e a pessoas jurídicas por diferentes autoridades certificadoras que, por sua vez, podem ser públicas ou privadas. O sistema oficial brasileiro de certificação digital baseia-se na ICP-Brasil – Infra-Estrutura de Chaves Públicas Brasileira, regulamentada pela Medida Provisória 2200-2, de agosto de 2001. Ela foi instituída para “garantir a autenticidade, a integridade, a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras”. O ITI é a Autoridade Certificadora Raiz da estrutura.

De acordo com a Medida Provisória, a organização da matéria é composta por uma autoridade gestora de políticas – o Comitê Gestor da ICP-Brasil – e pela cadeia de autoridades certificadoras, composta pela Autoridade Certificadora Raiz (AC-Raiz), pelas Autoridades Certificadoras (AC) e pelas Autoridades de Registro (AR). O Comitê Gestor é composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante dos ministérios da Justiça; da Fazenda; do Desenvolvimento, Indústria e Comércio Exterior; do Planejamento, Orçamento e Gestão; da Ciência e Tecnologia; da Casa Civil da Presidência da República e do Gabinete de Segurança Institucional da Presidência da República.

O Comitê Gestor estabeleceu o padrão tecnológico mínimo para emissão da certificação digital, e os pré-requisitos para que órgãos públicos ou privados se tornem autoridades certificadoras credenciadas. O sistema dá validade jurídica a documentos enviados por e-mail e a transações feitas pela internet que estejam com certificação. Atualmente, estão cadastradas pela ICP/Brasil para atuar como autoridades certificadoras as seguintes entidades: Presidência da República, Serpro, Serasa, CertiSign, Caixa Econômica Federal e Secretaria da Receita Federal.

O advogado Fabiano Menke comenta, em artigo sobre Interoperabilidade Aplicada à ICP, “o acerto da posição adotada pelo Brasil” na aprovação da



Medida Provisória: “Sem proibir que o mercado (aqui entendido como o conjunto dos agentes não estatais) implante soluções que possam vir a ser díspares no sentido de não direcionadas à coletividade, decidiu-se por fundar uma espinha dorsal normativa comum, um tronco ou, mais precisamente, uma árvore invertida, situando no topo (na raiz da árvore invertida) uma entidade de direito público, a autarquia federal Instituto Nacional de Tecnologia da Informação - ITI, com as atribuições principais de auditar, credenciar e fiscalizar as autoridades certificadoras, autoridades de registro e prestadores de serviços de suporte que integram a ICP-Brasil”.

O advogado, que é mestre em Direito Especial – Efeitos Jurídicos da Assinatura Digital –, comenta outros benefícios de uma estrutura nacional: “Havendo uma ICP mais abrangente, como são a brasileira e a alemã, torna-se bem mais viável e atraente a celebração de acordos internacionais de reconhecimento recíproco de certificados digitais, o que possibilitará transações eletrônicas internacionais mais seguras entre empresas e entre consumidores e empresas”.

Está em tramitação no Congresso Nacional o Projeto de Lei 7316/2002, que disciplina o uso de assinaturas eletrônicas e a prestação de serviços de certificação. A necessidade e urgência de aprovação dessa Lei são defendidas pelo diretor de Infra-Estrutura de Chaves Públicas do ITI, Renato Martini: “O maior mérito é institucionalizar uma estrutura que está funcionando operacionalmente. O Brasil vai ganhar uma Lei para disciplinar a questão”, afirma. “A Lei é flexível, pode ser alterada, ao contrário da Medida Provisória; pode sofrer emendas e se adaptar à evolução da sociedade. É muito importante uma Lei disciplinando a questão da certificação digital e da estrutura de chaves públicas”, garante. O Projeto de Lei tem como relator o deputado federal Jorge Bittar.

(Confira, nesta edição, na seção “Diálogo” - página 4 - entrevista com o advogado-geral do Estado de Minas Gerais, José Bonifácio Borges de Andrada, abordando, dentre outros aspectos, a questão legal da certificação digital no País).

Pensar nos benefícios da Certificação Digital significa, em resumo, pressupor a falta de riscos no ambiente vir-

tual, uma vez que a tecnologia utilizada no processo coíbe a ação de hackers na adulteração ou interceptação de documentos ou mensagens eletrônicas. Como um documento selado, evita-se, inclusive, a leitura de conteúdos por pessoas não autorizadas.

Facilidades como essas têm ampliado de forma expressiva o seu uso: segundo Sérgio Kulikovsky, há hoje aproximadamente 200 mil certificados emitidos em todo o território nacional, a maior parte para pessoas físicas, em uso profissional. “O número de certificados tem crescido muito”, avalia. “Neste ano, registramos cerca de 50% de crescimento em relação ao ano passado.” Para o ano que vem, a expectativa é de que esse número cresça ainda mais. “A previsão é de que teremos pelo menos 1 milhão de certificados emitidos em 2005.”

Esse crescimento se justifica, para Sérgio Kulikovsky, pelos investimentos que têm sido feitos na tecnologia que viabiliza seu uso. “A tendência é um rápido crescimento daqui para a frente; o mercado necessitava de uma série de requisitos de infra-estrutura, e têm sido feitas muitas implementações, que abrem agora uma boa perspectiva.”

“A popularização da certificação digital é fundamental para garantir a privacidade e os novos direitos na sociedade em rede”, afirma o diretor-presidente do ITI, Sérgio Amadeu da Silveira. “É, também, uma forma de dar mais segurança às transações eletrônicas. Atualmente, há vários projetos para dar mais segurança aos dados que transitam na rede. Podemos citar, como exemplo, uma política de divulgação, com utilização de mídia dirigida, eventos, entre outros, com o objetivo de tornar essa tecnologia mais conhecida.”

Em sua experiência à frente da CertiSign, Kulikovsky afirma que as resistências que se anunciavam no início do processo, em grande parte atribuídas à cultura do uso do papel, aos poucos vão dando lugar à aceitação de um recurso que tem se mostrado seguro. “Havia também o desafio da tecnologia, com relação à segurança e avaliação da possibilidade de risco” – lembra. “Mas, cada vez mais, as pessoas

vêm que esse tipo de questão não procede, elas vão se convencendo de que o recurso é, de fato, bom. Que vale a pena, desde que cercado das devidas precauções.”

O leque de empresas usuárias, representantes dos mais variados setores, se abre com a consolidação da tecnologia, contemplando principalmente aqueles que envolvem públicos de relacionamento numerosos, como é o caso das empresas públicas e do sistema bancário. O Sistema de Pagamentos Brasileiro, por exemplo, que movimenta diariamente milhões de reais entre os bancos, emprega de forma efetiva a certificação digital.

Da mesma forma, a Receita Federal se prepara para tornar ainda mais segura a relação com os contribuintes: brevemente, seus 25 mil servidores estarão utilizando certificados digitais, garantindo de forma mais eficaz o sigilo fiscal. A Receita investe também na segurança da Declaração de Imposto de Renda Retido na Fonte, trabalhando em conjunto com o ITI e bancos públicos e privados no projeto de emissão dos CPFs eletrônicos - E-CPF, que deverá contemplar todos os correntistas do País, substituindo o CPF em papel pelo eletrônico a médio e longo prazos. *(Detalhes na página 32).*

Governos estaduais descobrem nessa tecnologia a solução não só para a troca de documentos entre membros do alto escalão - no envio de conteúdos formatados eletronicamente para publicação em seus diários oficiais e tramitação burocrática de projetos de Lei -, mas, também, envolvendo contribuintes, como é o caso do Governo de Pernambuco, estado brasileiro pioneiro na adoção da tecnologia.

A Secretaria da Fazenda do Estado disponibilizou um conjunto de serviços pela internet, permitindo que os contribuintes inscritos sob regime normal de apuração cumpram com suas obrigações relativas às informações econômico-fiscais, aos benefícios fiscais do Prodepe - Programa de Desenvolvimento de Pernambuco - e à escrita fiscal mensal.

Na área jurídica, que trata com grandes volumes de papel na tramitação de documentos, a adoção da

certificação digital é recebida com empenho e bons resultados. O Tribunal de Justiça do Rio Grande do Sul já adota um sistema de informatização de sessões que permite que desembargadores redijam votos em seus gabinetes, compartilhem textos e emitam acórdãos com assinatura digital para publicação em tempo real na internet. No Rio de Janeiro, o Tribunal de Justiça implementa sistema para aumentar a segurança no uso de documentos resultantes de atos notariais.

Outro exemplo de sucesso é o Peticionamento Eletrônico adotado pelo Tribunal Regional de Trabalho/ 4ª Região, no Rio Grande do Sul, que tem proporcionado, desde junho de 2004, ganhos importantes para advogados e para o sistema. Segundo o diretor da Secretaria de Informática da entidade, Eduardo Kenzi Antonini, não há ainda mensuração matemática desses resultados, devido ao curto espaço de tempo desde sua implantação, mas o ganho em segurança é evidente, e a redução de custos para advogados de todo o Estado é drástica: “Não é necessário comparecer pessoalmente para entrega das petições; a economia de tempo e dinheiro com deslocamentos e hospedagens é expressiva. É importante destacar o aspecto da segurança da informação, pois não há extravio de documentos e garante-se a autenticidade e o não-repúdio, premissas que, num Tribunal, são essenciais”.

O serviço de Peticionamento Eletrônico ganha agora proporções nacionais, com o projeto E-Doc – Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos da Justiça do Trabalho –, que está em desenvolvimento, sob coordenação do TRT 4ª Região (*Detalhes na seção Benchmarking, página 33*).

O emprego da certificação digital ganha terreno também no comércio eletrônico, garantindo segurança aos compradores virtuais de produtos em sites seguros, identificados através da imagem de um cadeado; e nas áreas médica e odontológica, em prontuários virtuais.

Sérgio Kulikovsky identifica a generalização do uso da certificação, que já extrapola as entidades detentoras de grandes públicos de relacionamento, como bancos e seguradoras. Segundo ele, o Estado é um dos grandes usuários, mas profissionais liberais também já reconhe-



cem a importância da segurança em seus relacionamentos pela internet.

Opinião semelhante tem o diretor de Infra-Estrutura de Chaves Públicas do Instituto Nacional de Tecnologia da Informação, Renato Martini. Segundo ele, o poder público, através das aplicações do Governo Eletrônico, começa a se aproximar de um sistema de certificação digital. As máquinas financeira e bancária se apresentam mais organizadas e adiantadas que os governos. “Isso não é por acaso” – explica. “Reflete a conjuntura que criou a ICP, em 2001.”

Renato Martini explica: “O sistema financeiro tradicionalmente investe em tecnologia; portanto, para o setor, isso não é novidade. Quando se trata de usar a tecnologia para implementar segurança, isso também não é novidade. Já com as aplicações do Governo Eletrônico, não é tão fácil. São instituições que trabalham com tempos diferentes”.

Para Sérgio Kulikovski, um dos aspectos mais importantes de todo o processo, no momento, refere-se às perspectivas que a construção de uma infraestrutura tecnológica satisfatória viabiliza. Ele defende a opinião de que “o principal é poder oferecer mais serviços, para mais gente, de maneira menos burocrática e mais transparente”.

As restrições impostas pela falta de segurança - característica da rede mundial de computadores - limitaram, ao longo do tempo, a oferta de serviços, que acabaram por se perpetuar no papel. Sérgio Kulikovsky defende que o foco das empresas, a partir desse momento, deve estar nas possibilidades de ampliação de seu leque de produtos e serviços com base na segurança que a certificação agrega a quaisquer operações eletrônicas.

Para ele, “o grande desafio da certificação, agora, está na criação de aplicações úteis”. Ou seja, “pensar em quem vai usar, como e por que vai usar. O foco deve, portanto, ser deslocado da tecnologia para sua aplicação inteligente e útil, abandonando mitos e focalizando o usuário”.

## **Inclusão Digital - Inclusão Social**

Se a certificação digital representa a possibilidade de oferta de um número maior de novos serviços por um universo mais abrangente de empresas, o mesmo pode ser dito da ampliação dos usuários potenciais num segmento já tão elitizado? Na opinião do diretor do ITI, Renato Martini, sim. “Atualmente, não se pode falar de inclusão social sem associar a idéia da inclusão digital”, explica. “A tecnologia está presente fortemente em todos os setores e uma das ações políticas do Governo Federal é a popularização desse serviço. Todo cidadão que tiver uma conta bancária terá acesso. Se você populariza uma tecnologia, você promove a inclusão digital. A participação do cidadão brasileiro no uso de uma tecnologia de ponta promove naturalmente a inclusão social.”

A transparência que a certificação viabiliza para usuários detentores de um certificado é considerada, pelo presidente da CertiSign, um elemento de inclusão. “O cidadão passa a ter mais acesso ao que está acontecendo, pode acompanhar e até mesmo fiscalizar os serviços que são oferecidos. Isso significa que mais gente pode ter acesso a mais informações”, afirma. Com relação à indisponibilidade de microcomputadores em domicílios de baixa renda, Kulikovsky argumenta: “Não é necessário que você tenha um computador. Com o smart card ou token (mídias portáteis), o cidadão pode ter acesso a serviços e informações a partir de qualquer lugar, de qualquer computador. Você é você em qualquer lugar onde esteja. Você deixa de ser uma senha e passa a ser você de fato; passa a ser parte do processo”.

## **Interoperabilidade**

Garantir que todos os equipamentos que compõem a infra-estrutura da certificação digital no Brasil se comuniquem, independente do modelo, fabricante ou procedência, tem sido uma preocupação das autoridades envolvidas no processo. Para o advogado Fabiano Menke, “a interoperabilidade é um atributo necessário a qualquer infra-estrutura que

pretenda atingir a coletividade”.

Na sua opinião, em artigo sobre o tema, “a idéia que influenciou a criação da ICP-Brasil foi justamente a de construir uma infra-estrutura para a coletividade, para toda a sociedade, tornando mais facilitada a comunicação entre os titulares de certificados digitais”. Ele defende a necessidade de padronização, “a fim de que, na prática, se tenha a possibilidade de assinar digitalmente, bem como verificar as assinaturas digitais a partir de qualquer equipamento”. (*Leia artigo de Fabiano Menke sobre o assunto na página 39*).

Nesse sentido, o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira aprovou, no dia 21 de outubro, através da Resolução nº 36, o regulamento para homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil. A condução do processo será feita pela Autoridade Certificadora Raiz da ICP-Brasil, o Instituto Nacional de Tecnologia da Informação - ITI, e contempla mídias como tokens criptográficos e smart cards, sistemas como de assinatura eletrônica, de autenticação de assinatura, de autoridades certificadoras e de registro, e equipamentos como os de HSM, sincronismo e carimbo de tempo, entre outros.

Segundo o diretor-presidente do ITI, Sérgio Amadeu da Silveira, “a implementação de um laboratório que checará e homologará os dispositivos de segurança, como smart cards, que suportam os certificados, é uma iniciativa relevante. Já que, a partir dessa checagem, teremos certeza, seja qual for o fabricante do dispositivo, de que ele será interoperável, ou seja, aceito em todos os sistemas. Essa iniciativa reduzirá os custos dos certificados, facilitando a sua utilização em escala. O Governo, também, tem feito um esforço de utilizar essa tecnologia como forma de reduzir o trâmite de papéis e dar rapidez aos processos”.

O estabelecimento de padrões e especificações técnicas mínimas garantirá, portanto, a sua interoperabilidade e a confiabilidade dos recursos de segurança da informação. De acordo com a Resolução, os produtos homologados terão um laudo de conformidade emitido e utilizarão o selo de homologação e seu correspondente número de identificação. Para isso, já foi inaugurado, em novembro, o primeiro Laboratório de Ensaios e Auditoria –



LEA, em São Paulo, numa parceria do ITI com o Laboratório de Sistemas Integráveis – LSI da Escola Politécnica da USP. O LEA será responsável pela homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil.

### **Chaves Públicas**

O sistema de chaves públicas prevê a certificação através de duas chaves, uma chave privada – do seu proprietário, o remetente – utilizada para assinar o documento; e uma chave pública, de conhecimento geral, que validará a assinatura, consolidadas ambas num certificado digital.

O que garante segurança ao processo é justamente a autoridade certificadora, uma terceira entidade presente no processo, que atesta para o destinatário que o remetente é quem de fato assina o documento. O processo de emissão de um certificado pressupõe o reconhecimento pessoal do interessado em ter seu certificado pela entidade certificadora. Funciona, em outras palavras, como uma assinatura reconhecida em cartório pelo tabelião, que assegura que determinada assinatura pertence de fato àquela pessoa.

A tecnologia adotada é a criptografia assimétrica. Isso quer dizer que é impossível identificar o código de uma das chaves a partir da outra. Outra característica é o fato de uma chave desempenhar exatamente função inversa à outra: uma delas – a privada – é usada para assinar o documento; a outra, a chave pública, é utilizada para reconhecer a autenticidade da assinatura.

A criptografia assimétrica se distingue da criptografia simétrica: neste caso, ambos – remetente e destinatário – conhecem o algoritmo utilizado para criptografar a mensagem, o que a torna menos segura.

As chaves garantem não só a autenticidade da assinatura, mas também a comunicação segura para troca de documentos e mensagens. Um dispositivo, o “algoritmo de hash”, é capaz de acusar qualquer

interferência na mensagem em seu trânsito entre o remetente e o destinatário.

### **Assinatura Eletrônica x Assinatura Digital**

O professor Fabiano Menke define de forma esclarecedora a diferença básica entre a assinatura eletrônica e a assinatura digital. Insere-se na primeira categoria qualquer meio para identificar o remetente de uma mensagem, como a assinatura escaneada ou digitalizada. Mesmo que a ela sejam associados outros atributos - como digitais, íris, voz - é facilmente editável, estando portanto mais sujeita a fraudes.

Já a assinatura digital é algo mais, por associar inequivocamente uma pessoa a um documento, um código exclusivo a uma pessoa. Baseia-se na criptografia assimétrica – uma parte é privada e outra é pública –, ao contrário da criptografia simétrica, em que ambas as partes compartilham um código. Pressupõe ainda uma autoridade certificadora.

### **Governo Mineiro Adota Certificação Digital**

A administração pública em Minas conta com os benefícios da tramitação de documentos e informações pela internet de forma segura, através da tecnologia de certificação digital. A Companhia de Tecnologia da Informação de Minas Gerais - Prodemge - é a Autoridade Certificadora em Minas, coordenando um dos principais projetos previstos no Programa de Governança Eletrônica do Governo do Estado.

A adoção da tecnologia no Governo de Minas foi feita dentro dos parâmetros estabelecidos pela ICP-Brasil, portanto, orientada por padrões internacionais, que colocam a administração pública mineira em condições de se relacionar virtualmente com entidades de todo o mundo.

Para emitir os certificados, a Prodemge adequou sua infra-estrutura às exigências da ICP-Brasil. Foi feito processo de licitação para contratação de uma autoridade certificadora denominada de primeiro nível

– a CertiSign foi a vencedora - que hospeda em suas instalações os utilitários e o ambiente de segurança necessários, eliminando, num primeiro momento, a necessidade de grandes investimentos para montagem da estrutura. A equipe técnica da Prodemge também desenvolveu as aplicações de suporte ao serviço.

Para o diretor do ITI, Renato Martini, a Prodemge reflete hoje a aplicação da certificação digital no serviço público: “A empresa inteligentemente escolheu um dos cenários possíveis dentro dos parâmetros do ICP, ao aproveitar uma estrutura já existente, que custou grandes investimentos ao Governo e à sociedade”. Ela poderá, como AC, cadastrar, fazer a identificação física para emissão do certificado e ter o certificado para usar em seus procedimentos dentro do Governo. “Em um outro momento, a Prodemge poderá optar por evoluir para atuar como autoridade certificadora de primeiro nível”, explica Martini. “Nesse caso, é necessária a montagem da estrutura que exige grandes investimentos, como a sala-cofre e uma estrutura complexa de criptografia. Há cenários diferentes, a regulamentação da ICP é bastante flexível, oferecendo várias possibilidades.”

A adoção da certificação digital pelo governo mineiro representa um importante passo na modernização do Estado, ao eliminar de forma substancial a necessidade da tramitação de papéis.

Os primeiros projetos de certificação digital desenvolvidos são para a Junta Comercial do Estado de Minas Gerais – Jucemg – para envio eletrônico de livros mercantis, com significativa redução da tramitação de papéis e agilização do processo. Outra aplicação é da Secretaria de Estado de Planejamento e Gestão, e abrange todo o processo de tramitação de atos normativos do Governo provenientes da Secretaria, utilizando ferramenta de workflow. A Secretaria de Governo do Estado passa a contar com o Sistema Integrado de Processamento de Atos - SIPA -, destinado aos atos de provimento de cargos comissionados. A assinatura digital para responsáveis por esses atos representa também mais agilidade e economia na tramitação de papéis.

Outras aplicações que se beneficiarão de forma efetiva do serviço são a tramitação de informações e documen-

tos da Secretaria da Fazenda com os contribuintes do ICMS; a gestão eletrônica de documentos da Junta Comercial, que representa grandes volumes de papel; o relacionamento da Secretaria de Planejamento e Gestão com os fornecedores de serviços e produtos para o Estado; o envio de documentos oficiais para publicação pela Imprensa Oficial do Estado e a identificação segura de usuários dos sistemas corporativos do Estado, entre várias outras.

## **Empresas públicas estaduais e a certificação digital**

O Instituto Nacional de Tecnologia da Informação - ITI vem trabalhando com as empresas da ABEP – Associação Brasileira de Empresas Estaduais de Processamento de Dados-, a fim de consolidar a tecnologia junto aos governos estaduais. Segundo o diretor do Instituto, Renato Martini, já foram promovidos encontros em Brasília, com o presidente do Conselho da entidade, Marcos Vinícius Ferreira Mazoni, e com os presidentes das empresas estaduais de processamento de dados em Florianópolis, na última edição do Secop – Seminário Nacional de Informática Pública.

O ITI conduz um projeto de comunicação que visa a esclarecer o tema para as áreas públicas estadual e municipal. “Entendemos que a entrada da certificação digital para o serviço público é através das empresas estaduais de informática e chamamos a Abep para ser protagonista nesse processo, através de uma ação coordenada que contribua para a institucionalização do projeto.” Martini argumenta que é importante que as empresas públicas se organizem para ter um padrão, se coordenem e desenvolvam um projeto coletivo.

Para ele, trata-se de uma tecnologia complexa. “Daí a importância de explicar ao gestor público o seu funcionamento e benefícios. Estamos fazendo contato com os profissionais da área pública. Pernambuco tem hoje seus procedimentos fazendários baseados na certificação digital. Foi o Estado que saiu na frente. Há também boas iniciativas no Poder Judiciário. Mas é possível perceber um

desnível no conhecimento e aplicação da certificação digital entre os estados – alguns muito avançados, outros, não.”

O projeto do ITI busca justamente levar ao gestor público esse conhecimento. “Estamos elaborando guias, manuais, com conteúdo esclarecedor e texto de fácil entendimento.” O material será produzido pela Universidade Federal de Santa Catarina, que tem convênio com o ITI.

## **Dicas do ITI para maior segurança na utilização da certificação digital**

(fonte: site do ITI)

Primeiramente, deve-se lembrar que o certificado digital representa a “identidade” da pessoa no mundo virtual. Assim, é necessária a adoção de alguns cuidados para se evitar que outra pessoa possa praticar negócios jurídicos, acessar páginas na internet e realizar transações bancárias em nome do titular do certificado. Recomendações para o uso de um certificado digital:

- a senha de acesso da chave privada e a própria chave privada não devem ser compartilhadas com ninguém;
- caso o computador onde foi gerado o par de chaves criptográficas seja compartilhado com diversos usuários, não é recomendável o armazenamento da chave privada no disco rígido, pois todos os usuários terão acesso a ela, sendo melhor o armazenamento em disquete, smart card ou token;
- caso a chave privada esteja armazenada no disco rígido de algum computador, deve-se protegê-lo de acesso não-autorizado, mantendo-o fisicamente seguro. Nunca deixe a sala aberta quando for necessário sair e deixar o computador ligado. Utilize também um protetor de tela com senha. Cuidado com os vírus de computador, eles podem danificar sua chave privada;
- caso o software de geração do par de chaves permita optar entre ter ou não uma senha para prote-

ger a chave privada, recomenda-se a escolha pelo acesso por meio de senha. Não usar uma senha significa que qualquer pessoa que tiver acesso ao computador poderá se passar pelo titular da chave privada, assinando contratos e movimentando contas bancárias. Em geral, é bem mais fácil usar uma senha do que proteger um computador fisicamente;

- utilize uma senha longa, com várias palavras, uma vez que existem programas com a função de desvendar senhas. Deve-se evitar o uso de dados pessoais como nome de cônjuge ou de filhos, datas de aniversários, endereços, telefones ou outros elementos relacionados com a própria pessoa. A senha nunca deve ser anotada, sendo recomendável sua memorização.

## Como verificar uma assinatura digital?

Fonte: site da CertiSign

**Antes de confiar no conteúdo de um e-mail assinado digitalmente, você precisa verificar se o certificado utilizado para assiná-lo é legítimo. Nesse caso, a assinatura é verdadeira e você pode confiar no conteúdo da mensagem que recebeu, pois ela realmente foi enviada pela pessoa ou empresa que a está assinando.**

**Não ter esse cuidado pode significar confiar numa mensagem falsa, fraudada, em nome da pessoa ou empresa que a está assinando. Por isso, é importante verificar sempre a validade da assinatura digital antes de confiar nos e-mails e newsletters que você recebe.**

**Certificado válido significa assinatura verdadeira.**

**O procedimento de verificação é diferente para cada programa de e-mail.**



## Webmail

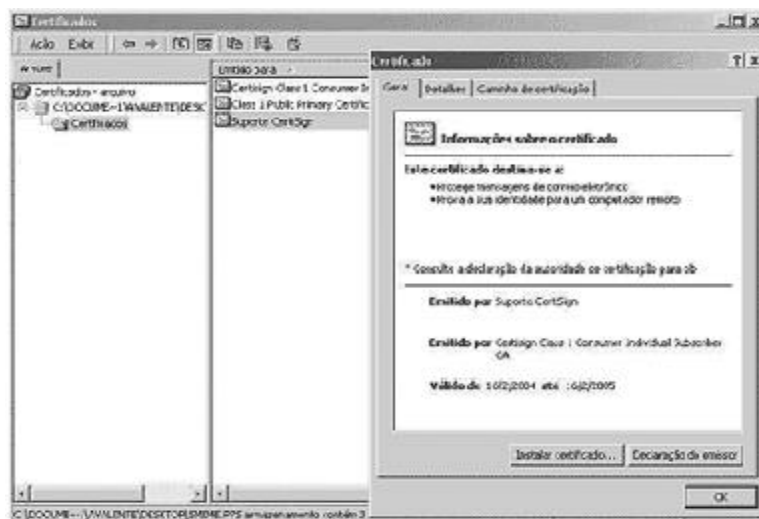
Quando recebemos um e-mail assinado digitalmente através de um webmail, o mesmo entende que a assinatura digital é um mero arquivo anexo (Smime.p7s) conforme a imagem abaixo:



Para poder verificar essa assinatura, você pode clicar no arquivo anexo e salvar o mesmo em sua área de trabalho.



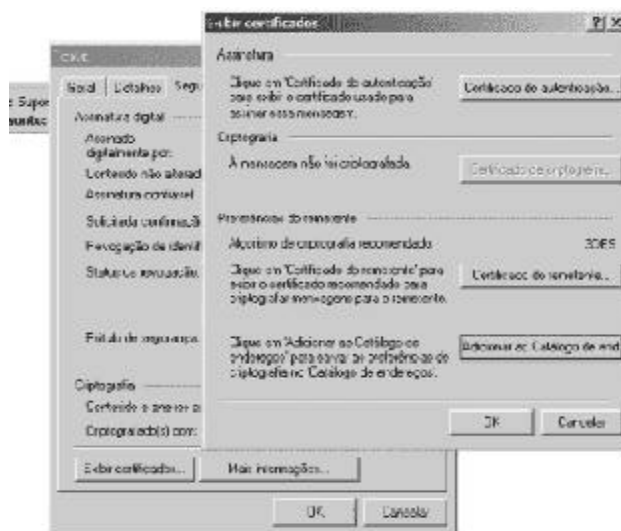
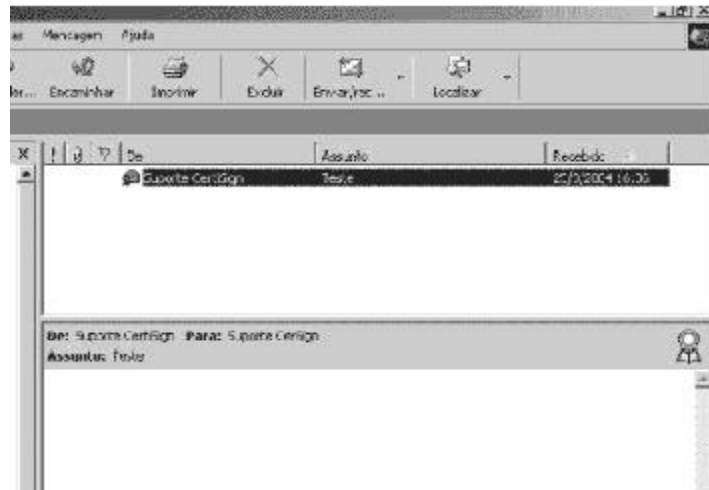
Após ter salvo o arquivo, você poderá dar um duplo clique no mesmo e verificar a assinatura digital que foi utilizada para assinar o e-mail que lhe foi enviado.





## Outlook

Ao receber um e-mail assinado, você irá visualizar uma chancela em vermelho no e-mail recebido.



Para verificar a assinatura do emissor, você deve clicar na mesma e, em seguida, nas opções "Exibir certificados" - "Certificado de autenticação".

Em seguida, lhe será mostrado o certificado digital que foi utilizado para assinar a mensagem.



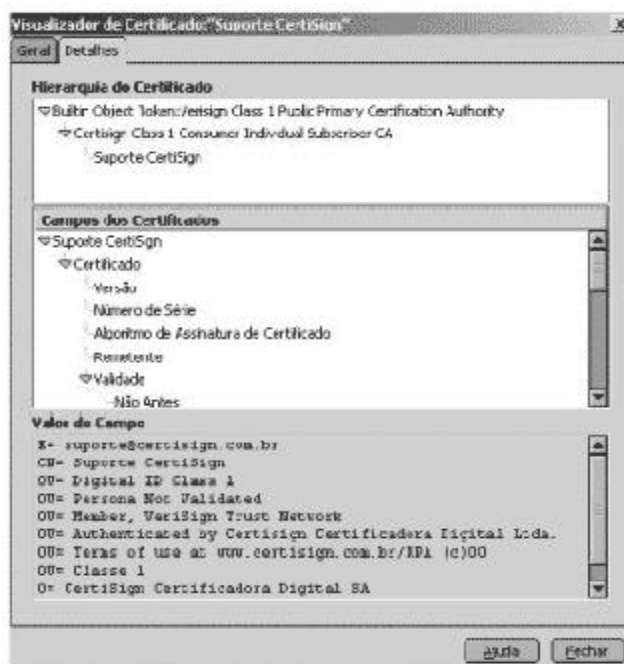
## Netscape

Ao receber um e-mail assinado utilizando o NetScape, você poderá visualizar uma “caneta” no cabeçalho da mensagem, representando que a mesma foi assinada digitalmente.



Para que você possa verificar a assinatura digital contida na mensagem, você deve clicar duas vezes neste ícone “Caneta” que a mesma irá lhe mostrar os dados referentes à certificação digital.

Para que você consiga todas as informações referentes a este certificado, você deverá clicar em “Exibir Certificado de Assinatura”.



## Glossário

**Autenticidade:** garantia de que a mensagem foi enviada por um remetente determinado e de que não é possível que outra pessoa se passe por ele.

**Autoridade Certificadora:** entidade autorizada a emitir certificados que vinculem uma determinada chave pública ao seu titular. Tem ainda outras atribuições, entre elas suspender, renovar ou revogar certificados digitais e emitir listas de certificados revogados.

**Confidencialidade:** atributo da mensagem protegida que garante que, após enviada, só será lida pelo destinatário e mais ninguém.

**Criptografia:** ramo das ciências exatas que tem como objetivo escrever em cifras. Trata-se de um conjunto de operações matemáticas que transformam um conteúdo em um texto cifrado.

**Garantia de Autoria:** presunção de que a mensagem é de fato assinada pela pessoa que se identifica.

**Interoperabilidade:** é pressuposto de uma infra-estrutura e pode ser definida como a capacidade que possuem os aparelhos e equipamentos que dela fazem parte de comunicarem-se entre si, independentemente de sua procedência ou de seu fabricante. (Fabiano Menke)

**Integridade:** garantia de que a mensagem que chega ao destinatário é exatamente a mesma que saiu do remetente, não tendo sofrido qualquer alteração em nenhuma de suas partes.

**Não-repúdio:** garantia de que o titular do certificado e autor da mensagem não pode negar a autoria de determinado documento. Numa situação assim, será dele o ônus de comprovar que seu certificado foi utilizado indevidamente.

**PKI:** tradução da expressão inglesa Public-Key Infrastructure - Infra-Estrutura de Chaves Públicas

**Token e smart card:** são hardwares portáteis que funcionam como mídias armazenadoras. Em seus chips, são armazenadas as chaves privadas dos usuários.

### Saiba Mais

---

Instituto Nacional de Tecnologia da Informação  
[www.iti.br](http://www.iti.br)

---

Infra-Estrutura de Chaves Públicas  
[www.icpbrasil.org](http://www.icpbrasil.org)

---

Companhia de Tecnologia da Informação do Estado  
de Minas Gerais  
[www.prodemge.mg.gov.br](http://www.prodemge.mg.gov.br)

---

CertiSign  
[www.certisign.com.br](http://www.certisign.com.br)

---

Tribunal Regional do Trabalho 4ª Região  
[www.trt4.gov.br](http://www.trt4.gov.br)

---

Módulo Security  
[www.modulo.com.br](http://www.modulo.com.br)

**Embora ainda em fase de consolidação no País, o uso da certificação digital ganha espaço em importantes setores da prestação de serviços públicos.**

**A seção Benchmarking mostra dois exemplos de projetos abrangentes e suas perspectivas para um número considerável de cidadãos brasileiros.**

# Receita Federal



Os 25 mil funcionários da Receita Federal, em todo o País, já se integram à crescente parcela de usuários da certificação digital. O órgão investe ainda na adoção dessa tecnologia para os contribuintes, ampliando o leque de serviços oferecidos pela internet, através do e-CPF ou CPF eletrônico, certificados digitais emitidos com a chancela do ICP-Brasil e que viabilizarão outro importante projeto: o Serviço Interativo de Atendimento Virtual, através do qual o contribuinte terá acesso, pelo computador, a serviços prestados atualmente apenas de forma presencial.

O projeto é conduzido em parceria com o ITI e bancos públicos e privados, para emissão de CPFs eletrônicos, que substituirão, a médio e longo prazos, o CPF em papel. As instituições bancárias deverão emitir um smart card contendo o certificado digital do cliente, com chancela da ICP-Brasil e o número de CPF do correntista. Esse talvez seja o mais

abrangente projeto em andamento no País, considerando-se o número de correntistas de bancos e a capilaridade das instituições bancárias.

Segundo o chefe da Divisão de Segurança da Informação da Receita Federal, Ariosto de Souza Júnior, a adoção da tecnologia para os funcionários e para os públicos de relacionamento da instituição se deve principalmente à consolidação da internet como canal de comunicação com o contribuinte: "Grande parte das informações com as quais lidamos são protegidas por sigilo fiscal, o que torna restrito o atendimento que podemos prestar se não tivermos a certeza de que o autor da demanda é efetivamente o contribuinte", explica.

Para ele, a certificação digital trará maior comodidade ao contribuinte, agilizará o atendimento aos processos e agregará maior segurança, consolidando, por

exemplo, um dos serviços importantes da Receita que é a entrega das declarações do Imposto de Renda: "Sem adotarmos a certificação digital, podemos receber as declarações via internet, mas alguns problemas que poderiam ser resolvidos remotamente acabam demandando o atendimento presencial, gerando desnecessárias filas nas delegacias da Receita".

Ele explica ainda como a tecnologia agregará agilidade ao processo: "Se recebemos um número cada vez maior de declarações via internet, a tendência é a Receita começar a dar encaminhamento aos processos todos de forma digital. Assim, por exemplo, quando um fiscal for analisar um processo, ele poderá assiná-lo eletronicamente com o seu e-CPF e aquele ato terá validade jurídica. A medida traz segurança aos sistemas informatizados da instituição e mais conforto também aos funcionários que, pelos métodos



tradicionais, têm que lembrar várias senhas para acesso a diferentes sistemas da Receita.

Ariosto de Souza Júnior lembra o processo de utilização da internet para oferta de produtos da Receita, que teve início em 1996, quando foram disponibilizadas somente a legislação tributária, informações de comércio exterior e trocas de informações com o contribuinte via correio eletrônico: “Em 97, a Receita disponibilizou o Recetanet, que é usado por 96% dos contribuintes brasileiros. Em 2004, o site da Receita registrou um total de 130 milhões de acessos e a entrega de 32 milhões de declarações. O serviço, que antes era utilizado apenas para a entrega das decla-

rações, já ampliou o atendimento a mais 120 outros documentos. Começamos então a disponibilizar serviços de consulta a aplicações, como a consulta à irregularidade fiscal e certidão negativa. Posteriormente, desenvolvemos aplicações para envio de dados como a declaração de isento, entre outras”.

A adesão dos usuários impôs, segundo Souza, a necessidade da implantação de novos recursos: “Avançamos até o limiar do que poderia ser oferecido sem ferir o sigilo fiscal. Como grande parte dos dados armazenados na Receita são protegidos por sigilo fiscal, chegamos no limite do que poderíamos fornecer sem a identificação do contribuinte”.

O processo de implantação da certificação digital passou pela aquisição de 27.500 smart cards, em fevereiro deste ano. Foram montados dois laboratórios de testes – um em Belo Horizonte, outro em Brasília –, além de um projeto piloto na Delegacia da Receita Federal em Contagem (MG). O projeto abrange 567 unidades da Receita Federal em todo o País.

“Usamos todo esse arranjo” – explica Ariosto Souza – “porque a Receita não quer aumentar o volume de atendimentos de balcão. Todo esse processo é para reduzir o atendimento presencial e facilitar a relação do contribuinte com a Receita”.



## **Tribunal Regional do Trabalho 4ª Região** **RIO GRANDE DO SUL**

No Rio Grande do Sul, o Tribunal Regional do Trabalho – 4ª Região implementou o primeiro sistema de Peticionamento Eletrônico do País, com adoção da certificação digital.

O serviço permite o envio eletrônico de petições através da internet, sem a necessidade da apresentação posterior dos ori-

ginais. A segurança da transação é garantida pela assinatura digital com utilização de certificados emitidos pela ICP-Brasil, que possuem validade jurídica de acordo com a Medida Provisória 2200-2.

Segundo o diretor da Secretaria de Informática do TRT, Eduardo

Kenzi Antonini, o projeto piloto foi desenvolvido com 20 advogados em dezembro de 2003 e, já em maio de 2004, o serviço foi ampliado para todos os interessados. Nos primeiros cinco meses do Peticionamento Eletrônico, cerca de 200 dos 8 mil advogados cadastrados no TRT4 já haviam adotado essa forma de trabalho.

Embora o pequeno tempo de uso do serviço não permita ainda medir com exatidão os seus resultados, o ganho em segurança e a redução de custos para advogados de todo o Estado é evidente. As vantagens se estendem também ao jurisdicionado, que ganha em rapidez e segurança; e ao sistema do judiciário, que ficou mais seguro - não há extravio de documentos -, ágil e simples. A autenticidade e o não-repúdio são, afinal, premissas essenciais num Tribunal.

### **Como funciona**

O TRT4 permite o envio de petições ao Tribunal e a todas as Varas do Trabalho da 4ª Região. Não estão contempladas no serviço as petições iniciais de 1ª instância e/ou seus aditamentos.

Em primeiro lugar, o usuário deve adquirir um certificado digital de qualquer entidade credenciada à ICP-Brasil. Para efetivar seu cadastro, é só acessar um formulário na internet e preencher os dados requisitados. No site do Tribunal, é possível fazer o download do Assinador Eletrônico; uma vez instalado no computador do usuário, o programa deverá ser usado para assinar eletronicamente suas petições, antes de enviá-las ao TRT.

Os arquivos são criptografados durante o envio. Ao receber a petição enviada eletronicamente,

o Tribunal analisa o arquivo recebido, verificando a validade da assinatura digital e se ela pertence efetivamente à petição enviada; consulta a data e a hora do recebimento junto ao Observatório Nacional; e gera um recibo da petição, que poderá ser impresso ou armazenado pelo advogado.

### **Projeto E-Doc**

O serviço de Peticionamento Eletrônico ganha agora proporções nacionais, com o projeto E-Doc – Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos da Justiça do Trabalho –, que está em desenvolvimento, a cargo do Grupo de Planejamento da Informatização da Justiça do Trabalho, coordenado pelo TRT da 4ª Região.

O objetivo é disponibilizar, através de infra-estrutura distribuída nos tribunais que compõem a Justiça do Trabalho, um sistema de envio e recebimento eletrônico de documentos aos Tribunais Regionais e ao Tribunal Superior do Trabalho. Da mesma forma que o Peticionamento Eletrônico do TRT4, será exigido o uso de certificados digitais emitidos pela ICP-Brasil, garantindo validade jurídica ao serviço.

Quando implantado, o E-Doc agregará ao sistema da Justiça do Trabalho mais agilidade e desburocratização, redução de custos e integração dos tribunais.

## Certificação Digital: o fim dos Cartórios?

**José Eisenberg**



A certificação digital – a atribuição de valor jurídico, através de criptografias personalizadas, para assinaturas enviadas através da rede mundial de computadores – apresenta um desafio instigante para o futuro da burocracia pública e privada, tal qual ela se conformou ao longo da história do Brasil. O nosso sistema jurídico, herdeiro do sistema centralizado português e sua estrutura oligárquica de

certificação de assinaturas em papel, em particular no Direito Civil, distribui a autoridade pública de certificação no mundo privado através de um sistema de cartórios, funcional e geograficamente atribuído, onde ainda funcionam antigas instituições de parentesco na reprodução do exercício daquela autoridade.

Para a economia, os cartórios representam simultaneamente custos de transação, a serem devidamente incluídos na formação de preços, e segurança para essas mesmas transações, em caso de litígios. Para o Direito, eles são entidades privadas investidas de autoridade pública cuja certificação confere validade a um documento envolvendo uma ou mais partes de um processo. Já para os cidadãos, os cartórios em geral representam uma senha para uma nova fila, uma taxa que subiu de novo, uma cópia autenticada da identidade que não ficou boa, ou, no caso dos mais afortunados, finalmente a escritura lavrada de uma casa própria.

A certificação digital, no modelo regulamentado pela ICP-Brasil (Infra-Estrutura de Chaves Públicas) na Medida Provisória 2200-2 de 8/2001, criou uma estrutura hierárquica de autoridades certificadoras, centralizadas em uma autoridade certificadora raiz

e regulada por uma nova agência, o Comitê Gestor da ICP-Brasil. As autoridades certificadoras, bem como as autoridades de registro abaixo delas, formarão um mercado que será regulado por esta agência, sendo cada ente auditado, credenciado e fiscalizado por uma entidade de direito público, o Instituto Nacional de Tecnologias de Informação (ITI), a autoridade certificadora raiz. Hoje ainda testemunhamos os

primeiros passos no sentido da implementação desse sistema, já que são em torno de seis autoridades certificadoras, sendo a maioria órgãos vinculados à União.

Para a economia, a certificação digital representa uma potencial diminuição dos custos de transação que resultam das prerrogativas de certificação dos cartórios. Amplia-se um mercado de certificação de documentos, mais moderno tecnologicamente e mais ágil do ponto de vista do tempo de transação, que certamente fará com que pessoas jurídicas, com cada vez mais frequência, incorram nos custos iniciais de investimento em uma estrutura de certificação digital (seja um *token*, um *smart card* ou uma chave no PC) para poder agilizar e diminuir os custos dessas transações. Em transações internacionais, em particular, ter acesso à certificação digital já está se tornando um imperativo.

Quanto à segurança das transações econômicas, ela será indubitavelmente maior. Uma criptografia assimétrica não é mais manipulável e/ou perigosa do que um carimbo, um selo ou uma rubrica de escrivão de cartório. Há certos mitos sobre as novas tecnologias de informação e comunicação que precisam ser abertamente combatidos e este é um deles.

Computadores são uma das formas mais seguras de armazenamento de informação já concebidas pela humanidade.

Já para o Direito, a certificação digital pode possibilitar uma verdadeira revolução no sistema processual. Com o grau de segurança e sigilo que a internet hoje permite, a certificação digital pode contribuir de forma decisiva para que os tribunais brasileiros esvaziem suas estantes e arquivos de processos. Desde acórdãos com assinatura digital publicados on-line, até a tramitação interna mais cotidiana de processos e seus documentos, a assinatura digital pode ser um instrumento vital que faltava ao Direito brasileiro para que ele, finalmente, converta sua rica estrutura de processamento de litígios e de garantia de direitos em uma ágil rede de interações capaz de mobilizar a capilaridade social de nossos tribunais em práticas democráticas de acesso à justiça para os menos favorecidos.

O sistema processual brasileiro certamente tem suas deficiências institucionais. Entretanto, a sua falta de celeridade resulta primordialmente de um aparato burocrático pouco preparado para acomodar as demandas advindas da sociedade, bem como a energia investigativa de um Ministério Público ativo e independente. Ainda que a informatização não tenha atingido a vasta malha de tribunais de justiça no Brasil, qualquer medida que leve o Estado a fazer os investimentos necessários para tornar o judiciário mais ágil deve ser louvada. Particularmente, se ela aumenta, simultaneamente, o grau de transparência das suas atividades.

Para os cidadãos, no curto prazo, tudo que diz respeito à certificação digital não passa de conversa de gente que mexe com computador. No longo prazo, porém, a inclusão digital é um problema educacional estrutural da sociedade brasileira que precisa ser atacado com políticas públicas dirigidas, porém universais, para que as novas gerações de brasileiros estejam devidamente equipadas com os instrumentos necessários ao pleno exercício da cidadania. A certificação digital é somente mais um prenúncio da premência desta outra agenda já que, caso ela se

consolide e encontre tanto no mercado quanto no poder público a receptividade e atenção que merece, não demorará muito para que nós passemos a ser uma sociedade dividida entre os com-CPF e os sem-CPF, mas também entre os que têm ou não assinatura digital. Seria ela o Registro Geral (R.G.) do futuro?

A grande virtude da Certificação Digital reside na possibilidade da descartorialização do nosso sistema de autenticação e certificação de transações entre entidades de direito civil, sejam elas pessoas físicas ou pessoas jurídicas. Abrir um mercado sem cartórios não é uma garantia contra a sua oligopolização (nem uma idéia tão inovadora assim nos tempos de hoje), mas faz sentido. Faz mais sentido ainda a centralização mantida na estrutura de autoridades constante na medida provisória aprovada sobre o assunto. Haverá sempre um problema de regulação desse mercado, e os agentes públicos e da sociedade civil precisam efetivamente operar nos diversos níveis da burocracia regulatória para agir como efetivos fiscalizadores da qualidade dos serviços de certificação digital oferecidos.

A segurança do sistema virá. Mas pairam dúvidas. Curiosamente, no dia 1º de novembro, a página do ITI para divulgação de seu 2º Fórum de Certificação Digital estava fora do ar, tendo sido invadida por um protesto que clamava "*Nós somos os fora-da-lei de uma lei que não existe*".

Todos, pelo jeito, até mesmo os invasores da página do ITI, aguardam a aprovação do Projeto de Lei 7316/2002, que disciplinará o uso de assinaturas eletrônicas e o mercado de certificação digital. Eu, de minha, parte, espero que, no longo prazo, possamos olhar para os passos que damos hoje como o começo do fim de uma era dos cartórios no Brasil.

**José Eisenberg** - Professor de Ciência Política (IUPERJ), é co-organizador de *Internet e Política: teoria e prática da democracia eletrônica* (Belo Horizonte: Ed. UFMG, 2001) e autor de vários artigos sobre novas tecnologias de informação e comunicação.



# Fonte

A Tecnologia da  
Informação na  
Gestão Pública

Dezembro de 2004

**Contribuições acadêmicas  
exclusivas, focadas nos  
temas certificação digital e  
segurança da informação**



UNIVERSIDADE  

---

CORPORATIVA  

---

P R O D E M G E



# Considerações sobre a interoperabilidade aplicada à infra-estrutura de chaves públicas



## Fabiano Menke

Advogado. Ex-procurador-geral do Instituto Nacional de Tecnologia da Informação. Membro da Comissão Técnica Executiva da Infra-Estrutura de Chaves Públicas Brasileira. Mestre em Direito pelo Curso de Pós-Graduação de Concentração em Direitos Especiais. Professor de Direito Civil no Centro Universitário Ritter dos Reis, Canoas, RS.

## RESUMO

O artigo analisa a interoperabilidade aplicada à Infra-Estrutura de Chaves Públicas (ICP). Principia delineando noção geral de interoperabilidade e, após, versa especificamente sobre a interoperabilidade existente numa ICP. Explica o significado da palavra “infra-Estrutura”, que é de fundamental importância para a análise do objeto de estudo. A abordagem é feita com ênfase na Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), instituída pela Medida Provisória nº 2.200. Além disso, apresenta a interoperabilidade como gênero que se divide em dois, a interoperabilidade formal, operacional, técnica ou objetiva, e a interoperabilidade substancial ou subjetiva.

*Palavras-chave:* interoperabilidade; infra-estrutura (de chaves públicas).

### 1. Noção geral de interoperabilidade

Uma noção geral de interoperabilidade pode ser obtida a partir de um exemplo prático, como o regulado pela Diretiva da Comunidade Européia nº 96/48, de 23 de julho de 1996, que trata da “interoperabilidade do sistema ferroviário transeuropeu de alta velocidade”. Nos considerandos dessa Diretiva, é dito: “para que os cidadãos da União, os operadores econômicos e as

coletividades regionais e locais se beneficiem plenamente das vantagens decorrentes da criação de um espaço sem fronteiras, importa, designadamente, incentivar a interconexão e a interoperabilidade das redes nacionais de trens de alta velocidade, bem como o acesso a essas redes”. Observe-se bem, a Comunidade Européia resolveu adotar uma diretiva estabelecendo critérios e padrões comuns para possibilitar que um trem francês possa sair de Paris, passar por cidades alemãs

e finalmente chegar a Viena, na Áustria, sem que no percurso encontre qualquer problema de incompatibilidade. Para atingir esse objetivo, foram criadas as ETI, que são as especificações técnicas de interoperabilidade, “a que cada subsistema é objeto a fim de satisfazer os requisitos essenciais, estabelecendo as necessárias relações funcionais recíprocas entre os subsistemas do sistema ferroviário transeuropeu de alta velocidade”.

Talvez esse exemplo seja o mais elucidativo para ilustrar o que seja, numa acepção mais geral, interoperabilidade. Por meio dele, verifica-se que a interoperabilidade é um apanágio necessário de qualquer infra-estrutura e pode ser definida como a capacidade que possuem os aparelhos ou equipamentos que dela fazem parte de comunicarem-se entre si, independentemente de sua procedência ou do seu fabricante. Num sistema de telefonia celular, por exemplo, a interoperabilidade permite que dois indivíduos que tenham aparelhos diversos e linhas telefônicas de operadoras diversas possam conversar sem problemas. O mesmo princípio se aplica a uma infra-estrutura de chaves públicas, ou seja, “A” poderá se comunicar eletronicamente com “B”, ainda que os seus certificados digitais e os equipamentos que utilizem para criar e verificar assinaturas digitais não

sejam fornecidos pelo mesmo fornecedor (aqui incluídos a respectiva autoridade certificadora emissora do certificado digital e os fornecedores de *hardware* e *software* utilizados para criar e verificar assinaturas).

## 2. Infra-Estrutura e ICP-Brasil

Não raro, os debates sobre os temas atinentes às assinaturas e certificados digitais fecham os olhos para uma característica fundamental de uma infra-estrutura de chaves públicas (ICP), qual seja, a de que, antes de tudo, e por mais pleonástico e óbvio que possa soar, uma ICP é uma infra-estrutura<sup>1</sup>. E por ser uma infra-estrutura é que a interoperabilidade lhe é ínsita. Portanto, seja qual for a infra-estrutura (de energia elétrica, de saneamento básico, de ferrovias, de telefonia fixa, de telefonia móvel, de chaves públicas, etc.), a palavra interoperabilidade, no mais das vezes, estará presente e dela será um atributo indispensável, sempre que o serviço fornecido tiver por escopo atingir a coletividade.

Insistindo no ponto, uma infra-estrutura de chaves públicas tem o mesmo princípio de qualquer outra instalação estrutural posta à disposição da sociedade, qual seja o de prover um serviço que pode ser obtido por qualquer interessado. Como é sabido, o termo infra-estrutura de chaves públicas é tradução da expressão da língua inglesa: *public-key infrastructure (PKI)*. Os norte-americanos bem souberam esclarecê-la, partindo, primeiramente, da própria definição da palavra infra-estrutura. **Carlisle Adams** e **Steve Lloyd**, na obra *Understanding Public-Key Infrastructure*<sup>2</sup> enfatizaram que uma infra-estrutura se caracteriza por

ser uma *pervasive substrate*, ou seja, uma fundação que dissemine algo para um amplo ambiente ou para um grande universo de interessados. Salientam que duas infra-estruturas comuns são a de comunicações eletrônicas e a de energia elétrica. Asseveram que o princípio de ambas é idêntico: a infra-estrutura existe para que qualquer usuário possa simplesmente acoplar-se a ela e dela fazer uso quando necessário.

A infra-estrutura uniforme evita que sejam aplicadas soluções díspares por cada entidade.

Quanto a esse ponto, é elucidativa a explicação de **Adams** e **Lloyd**: *"The pervasive security infrastructure is fundamentally the sensible architecture for many environments. This architecture avoids piecemeal, point-to-point, ad hoc, non-interoperable solutions, thereby introducing the possibility of manageable, consistent security across multiple applications and computing platforms. It is not difficult to imagine the chaos that would result from every pair of communicants running their own communications lines, or from every person running his/her own power generator at his/her own arbitrarily chosen voltage and current. Many facets of both ancient and modern society demonstrate that the uniformity and convenience offered by a well-designed, well-defined, pervasive infrastructure is worth the effort involved in the design and definition stages"*<sup>3</sup>.

Atente-se bem à observação contida no texto citado: uma infra-estrutura de segurança disseminada, uniforme, evita soluções díspares, isoladas, não interoperáveis. O exemplo fornecido do

caos que resultaria do fato de cada indivíduo operar as suas próprias linhas de comunicação ou de geração de energia é emblemático.

Daí, no meu entender, o acerto da posição adotada pelo Brasil no que toca ao modelo de infra-estrutura de chaves públicas escolhido por meio da Medida Provisória nº 2.200 e regulações posteriores. Sem proibir que o mercado (aqui entendido como o conjunto dos agentes não estatais) implante soluções<sup>4</sup> que podem vir a ser díspares no sentido de não direcionadas à coletividade, decidiu-se por fundar uma espinha dorsal normativa comum, um tronco ou, mais precisamente, uma árvore invertida (*inverted tree*)<sup>5</sup>, situando no topo (na raiz da árvore invertida) uma entidade de direito público, a autarquia federal Instituto Nacional de Tecnologia da Informação – ITI, com as atribuições principais de auditar, credenciar e fiscalizar as autoridades certificadoras, autoridades de registro e prestadores de serviços de suporte que integram a ICP-Brasil.

O modelo adotado pelo Brasil é idêntico ao alemão<sup>6</sup>. Lá, uma divisão do órgão regulador *Regulierungsbehörde für Telekommunikation und Post (Reg-TP)*, com natureza de direito público e vinculada ao Ministério da Economia e Tecnologia, desempenha o mesmo papel que o Instituto Nacional de Tecnologia da Informação, ou seja, credencia, fiscaliza e emite certificados digitais para os prestadores de serviços de certificação (*Zertifizierungsdiensteanbieter*) do primeiro nível hierárquico da cadeia. Até o presente momento, vinte e três *Zertifizierungsdiensteanbieter* já obtiveram credenciamento pe-



rante a RegTP. Entre os credenciados, encontram-se os correios (Deutsche Post), diversas empresas, as entidades de classe dos advogados, as representações de consultores fiscais<sup>7</sup>.

Curiosamente, há que se ressaltar que nos Estados Unidos da América o desenvolvimento e a expansão das infra-estruturas de chaves públicas se deu de forma bastante desorganizada, de sorte que hoje em dia são diversas as ICPs em funcionamento naquele país, com base tanto em iniciativas governamentais quanto em iniciativas privadas.

As razões desse fenômeno são diversas, sendo que um dos motivos principais é o fato de que a autonomia dos estados federados fez com que cada unidade da federação editasse a sua própria lei sobre assinaturas digitais e matérias afins, sem que houvesse uma harmonia principiológica permeando esses diplomas.

Todavia, cientes de que *"PKI is no good if you are only talking to yourself"*<sup>8</sup>, os norte-americanos há alguns anos promoveram a iniciativa do projeto *Federal Bridge Certification Authority*, que tem por escopo fundamental viabilizar a intercomunicação entre os titulares de pares de chaves cujos respectivos certificados sejam provenientes de autoridades certificadoras diversas. Em que pese os esforços, os próprios envolvidos no projeto têm reconhecido que a iniciativa se transformou numa "empreitada que tem sido marcada pelo lento progresso"<sup>9</sup>.

Daí a razão de ser mais racional e de resultados certamente melhores à implementação, desde o princípio, de uma ICP nacional.

Outro aspecto é que, havendo uma ICP mais abrangente, como são a brasileira e a alemã, torna-se bem mais viável e atraente a celebração de acordos internacionais de reconhecimento recíproco de certificados digitais, o que possibilitará transações eletrônicas internacionais mais seguras, entre empresas e entre consumidores e empresas<sup>10</sup>.

No Brasil, as normas a serem cumpridas e observadas pelo ITI e por todas as entidades integrantes da ICP-Brasil são deliberadas pelo Comitê Gestor, que tem na Comissão Técnica Executiva (COTEC) o seu braço técnico e órgão consultivo que examina todas as proposições a serem apreciadas<sup>11</sup>.

Dos estudos da COTEC, e das contribuições advindas da consulta pública realizada em 2001, é que se originaram os documentos básicos da ICP-Brasil, posteriormente aprovados pelo Comitê Gestor. Até o momento, já foram deliberadas cerca de trinta resoluções, mas aquelas que poderiam ser consideradas o núcleo duro normativo são as Resoluções de nºs 1, 2, 7 e 8 (respectivamente, Declaração de Práticas de Certificação da AC Raiz, Política de Segurança da ICP-Brasil, Requisitos mínimos para as Políticas de Certificados e Requisitos mínimos para as Declarações de Práticas de Certificação).

3. Interoperabilidade e ICP-Brasil: interoperabilidade objetiva e interoperabilidade subjetiva

Este conjunto de resoluções e a Medida Provisória nº 2.200-2 contém a base técnica e jurídica da infra-estrutura, e tem como um dos escopos principais garan-

tir a interoperabilidade na utilização dos serviços relacionados à certificação digital, a partir do estabelecimento de padrões<sup>12</sup>. E a idéia que influenciou a criação da ICP-Brasil foi justamente a de constituir uma infra-estrutura para a coletividade<sup>13</sup>, para toda a sociedade, tornando mais facilitada a comunicação entre os titulares de certificados digitais. Evidente que nem tudo está feito, pelo contrário, a implementação das assinaturas digitais certamente trará dificuldades e problemas e mostrará que há muito por fazer para que efetivamente se atinja a desejada interoperabilidade, que deve ser encarada como um desafio, algo em constante construção, e não como algo pronto e acabado, que tenha se esgotado com a simples edição do conjunto normativo mencionado.

E um desses desafios é o relativo à compatibilidade dos cartões inteligentes, leitoras e softwares. Esse ponto é fundamental. Há que se padronizar esses instrumentos, a fim de que, na prática, se tenha a possibilidade de assinar digitalmente, bem como verificar as assinaturas digitais a partir de qualquer equipamento. Por isso, há que se louvar a iniciativa do Instituto Nacional de Tecnologia da Informação em constituir, por meio da Portaria nº 33, de 8 de abril de 2003, grupo de trabalho "para o estudo de padrões com especificações mínimas para o uso de hardwares e softwares na Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil", que redigirá "minuta de resolução que será submetida ao Comitê Gestor da ICP-Brasil" e que tem como uma das finalidades "colaborar na interoperabilidade desses dispositivos"<sup>14</sup>. Realmente, este é um ponto essencial, mas não é só a partir dele

que se explica a interoperabilidade, que, a meu juízo, não termina aí. O que se verifica é que, além dessa interoperabilidade, que eu proporia a denominação de interoperabilidade operacional, formal, técnica ou objetiva, existe uma outra interoperabilidade, que se poderia cunhar de interoperabilidade substancial ou subjetiva. Enquanto que a primeira tem em mira a operação em si, ou seja, a própria criação da assinatura digital e a sua posterior verificação pelo destinatário do documento eletrônico, a segunda, a interoperabilidade subjetiva, vai um pouco além, ela invoca um fundo comum principiológico de índole normativa que faz com que os indivíduos envolvidos na comunicação ou transação eletrônica, seja como signatário, seja como *relying party*, confiem na utilização do serviço, sentindo-se seguros não só aqui e agora, ou seja, no momento da utilização do certificado digital, mas para trás e para frente, isto é, antes e depois de efetuada a transação eletrônica. A preocupação ora enfocada se dirige a aspectos outros, como os relativos aos critérios observados para identificar os titulares de certificados, à forma de geração do par de chaves criptográficas, direitos e obrigações das partes (deveres de indenizar, de contratação de seguro, etc.) e muitos outros que sustentam e regulam a operação técnica da utilização da assinatura digital.

O que se quer dizer com isso é que não basta que os dispositivos de criação e de verificação das assinaturas funcionem aqui e agora. Da mesma forma, não basta que todos os indivíduos envolvidos na transação ou na comunicação utilizem o padrão do formato do certificado X.509. Pre-

tender que a interoperabilidade se resolva apenas a partir da utilização disseminada do padrão X.509 é, sem dúvida, analisar o problema de forma bastante superficial e com total desconhecimento da magnitude envolvida nessa questão.

Por isso, dentre outras coisas, é importante que se tenha confiança de que aquele indivíduo que assinou digitalmente foi corretamente identificado pela autoridade de registro. Assim, Pedro deverá ser realmente Pedro, e não João. Aqui, portanto, vai um primeiro princípio, de suma importância, que é o da identificação do indivíduo mediante a sua presença física<sup>15</sup>, no sentido de tentar evitar, o máximo possível, as fraudes.

Outra norma importantíssima é a da geração do par de chaves pelo próprio titular do certificado, que tem por evidente finalidade evitar a alegação de rejeição da autoria de determinado documento eletrônico pelo titular do certificado, alcançando-se, assim, o denominado não-repúdio<sup>16</sup>. Poder-se-ia citar também as normas referentes ao tempo limite para revogação dos certificados e a frequência de emissão da Lista de Certificados Revogados (LCR)<sup>17</sup>.

Por outro lado, para que a interoperabilidade efetivamente se realize, é preciso que as aplicações que requeiram a utilização da certificação digital não restrinjam o acesso a certificado digital específico, isto é, emitido por apenas uma das autoridades certificadoras. Isso, evidentemente, para os casos de “aplicações voltadas para atendimento ao público em geral, assim considerados, dentre outros, os consumidores,

os contribuintes, os cidadãos, os beneficiários do sistema de saúde, do FGTS, da seguridade social (...)”<sup>18</sup>. Essa norma tem forte conotação de proteção do consumidor, para evitar, na medida do possível e da razoabilidade, que para cada aplicação se tenha que utilizar um certificado digital diferente.

Sem a pretensão de fazer um elenco exaustivo de todas essas regras que constituem esse fundo principiológico normativo comum, chama-se a atenção para um outro ponto, pouco falado, mas de fundamental importância, que é o contido no item 6.3.1 da Resolução nº 7 da ICP-Brasil, que se refere à obrigação das autoridades certificadoras de armazenar, pelo prazo mínimo de 30 anos, as chaves públicas dos titulares de certificados digitais já expirados. Esse é um item essencial. Por meio da observância dele, é possível que se verifique a assinatura digital muito tempo depois de ter sido assinado o documento eletrônico, o que é de suma importância naqueles casos em que se fará necessária a sua posterior apresentação e conferência. Esse prazo é mínimo, por vezes pode haver a necessidade de que as chaves públicas sejam armazenadas por tempo ainda maior<sup>19</sup>. O lapso temporal de 30 anos é devido ao prazo máximo prescricional que poderia haver na legislação. Vale lembrar que, na Alemanha, o certificado de uma autoridade certificadora credenciada é considerado imprescindível, entre outros tantos aspectos, porque há esta obrigação de armazenamento das chaves públicas, que também é de 30 anos a contar do primeiro dia do ano seguinte ao da expiração do certificado digital<sup>20</sup>. Para as entidades que não são creden-

ciadas, a obrigação é de, no mínimo, 5 anos<sup>21</sup>.

Conforme referido, existe, na ICP-Brasil, um sem-número de outros aspectos, tão ou mais importantes do que os alinhados, como a obrigatoriedade de contratação de seguro pelas autoridades certificadoras, segurança dos dispositivos de armazenamento da chave privada, segurança do ambiente físico das autoridades certificadoras, vedação do denominado *key-escrow*, procedimentos de auditoria e de fiscalização, que acabam por constituir esse fundo principiológico comum, de índole normativa, e que geram, ou devem gerar, nos indivíduos integrantes da estrutura e naqueles que utilizam ou conferem os certificados digitais, um sentimento de segurança, e, mais do que isso, a *confiança*, que talvez seja a palavra-chave de uma infra-estrutura de chaves públicas e que os alemães bem souberam utilizar ao qualificarem a sua, denominando-a de *Kette des Vertrauens* (cadeia, ou rede da confiança).

É verdade que nem todos os indivíduos, ao utilizarem o seu certificado digital, estarão conscientes de todos esses aspectos, e também é verdade que fraudes e erros ocorrerão, pois nenhum sistema é de todo imune à falhas, mas o importante é que os usuários tenham um mínimo de segurança e de discernimento de que o máximo foi feito para se evitar problemas, e que se, porventura, algum venha a ocorrer, alguém será responsabilizado, como na hipótese de uma autoridade certificadora encerrar definitivamente as suas atividades, caso em que outra entidade deverá assumir as suas funções, pelo menos no que toca aos certificados digitais já emitidos<sup>22</sup>. Oportuno des-

taçar aqui, também, a importância de o Estado regular e fiscalizar esse incipiente, mas promissor, mercado, haja vista que os consumidores ainda não têm um mínimo de consciência acerca do que significa e do que não significa qualidade no que toca à prestação dos serviços de certificação digital. Quanto a esse aspecto, recomendo expressamente a leitura da resposta número um das FAQs, contida na página da *Regulierungsbehörde für Telekommunikation und Post*<sup>23</sup>, onde é feito um paralelo entre as exigências dos consumidores, motoristas de automóveis, de vinte e cinco anos atrás, e as de hoje.

Assim, verifica-se que para haver interoperabilidade não basta que o simples procedimento da assinatura digital do momento, do aqui e do agora, funcione. É necessário que todo o sistema tenha funcionado satisfatoriamente desde a primeira identificação do primeiro titular de certificado e que continue a funcionar, indefinidamente, de forma razoável. Além disso, será muito difícil que se estabeleçam transações ou comunicações virtuais que demandem segurança se as pessoas naturais ou jurídicas não estiverem regidas e protegidas por um fundo principiológico comum que, além de lhes impor deveres, lhes transmita confiança na utilização do meio eletrônico. Em suma, é importante que os documentos básicos das autoridades certificadoras (as PC e DPC) contenham um mínimo de similaridade quanto aos aspectos primordiais dos serviços, a fim de que seja possível a “conversação”. Daí a importância dessa “outra perna” da interoperabilidade, que enfeixa todos os aspectos citados, que poderia ser chamada, para efeitos ilustrativos, de interopera-

bilidade substancial ou subjetiva.

#### 4. Conclusões

(a) a interoperabilidade é um atributo necessário de qualquer infra-estrutura que pretenda atingir a coletividade, e consiste, numa acepção geral, na capacidade que têm os aparelhos ou equipamentos que fazem parte dessa infra-estrutura de comunicarem-se entre si, independentemente de sua procedência ou do seu fabricante; assim como uma infra-estrutura ferroviária necessita de padrões, uma infra-estrutura de chaves públicas também deverá estabelecer *standards* mínimos a serem observados pelos seus integrantes;

(b) neste sentido, o modelo da ICP-Brasil, previsto na Medida Provisória nº 2.200-2, e que é idêntico ao adotado pela Alemanha e outros países, deve ser considerado razoável, uma vez que, com o estabelecimento de uma espinha dorsal normativa comum, resta bastante facilitada a interoperabilidade;

(c) a noção de interoperabilidade aplicada a uma infra-estrutura de chaves públicas não se esgota no simples funcionamento da criação da assinatura digital, numa ponta, e de sua verificação na outra; portanto, ao lado dessa interoperabilidade objetiva, formal ou operacional, há que se referir à interoperabilidade subjetiva ou substancial, que invoca um fundo principiológico comum, expressado nas normas e padrões, que conferem as necessárias confiança e segurança aos usuários dos serviços de certificação digital;

(d) enfim, a interoperabilidade é algo a ser permanentemente

construído, um desafio constante, que exige esforço de todos os envolvidos. Há, como se sabe, muito a ser feito na ICP-Brasil. Por fim, eu chamaria a atenção para um último ponto que exigirá regulação num futuro bem próxi-

mo e que, salvo meu desconhecimento, pouco tem sido abordado no Brasil com vistas a sua inserção na ICP-Brasil, que é o atinente à necessidade de se proceder a reassinatura (aposição de nova assinatura digital) nos do-

cumentos eletrônicos que necessitam arquivamento por longo período de tempo, tendo em vista que “os procedimentos de criptografia podem perder, ao longo dos anos, seus atributos de segurança”<sup>24</sup>.

---

## Notas

<sup>1</sup> A definição do vocábulo “infra-estrutura” do Dicionário Aurélio, no que toca à área de urbanismo, é a mais adequada à acepção ora enfocada, *in verbis*: “Numa cidade, o conjunto das instalações necessárias às atividades humanas, como rede de esgotos e de abastecimento de água, energia elétrica, coleta de águas pluviais, rede telefônica e gás canalizado.” Vide *Novo Aurélio Século XXI: o dicionário da língua portuguesa*, Aurélio Buarque de Holanda Ferreira. Rio de Janeiro: Nova Fronteira, 1999.

<sup>2</sup> Obra cujo subtítulo é *Concepts, Standards, and Deployment Considerations*. Indianapolis: New Riders, 1999. p. 27.

<sup>3</sup> Ob.cit. p.27-28.

<sup>4</sup> É o que se depreende do parágrafo segundo da Medida Provisória nº 2.200-2, de 24 de agosto de 2001: “O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação de autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados digitais não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento”.

<sup>5</sup> A comparação com a árvore invertida está na obra citada, página 134.

<sup>6</sup> Pelo que se tem notícia, além de Brasil e Alemanha ([www.regtp.de](http://www.regtp.de)), Coreia do Sul ([www.rootca.or.kr](http://www.rootca.or.kr)), Índia ([www.cca.gov.in](http://www.cca.gov.in)), Áustria ([www.rtr.at](http://www.rtr.at)), México e Japão apresentam o mesmo modelo hierárquico com uma entidade de direito público desempenhando o papel de Autoridade Certificadora Raiz. Quanto ao Japão e sua forte inspiração alemã, vide “*Japanische Signaturgesetzgebung – Auf dem Weg zu „e-Japan*”. Artigo de autoria de Alexander Roanagel e T. Yonemaru, Revista Multimedia und Recht, nº 5, volume 12, p. 798 – 806.

<sup>7</sup> Conferir em [www.regtp.de](http://www.regtp.de)

<sup>8</sup> São as exatas palavras proferidas por Peter Alterman, diretor de operações do escritório de pesquisa extra-mural do Instituto Nacional de Saúde dos Estados Unidos da América. Declaração contida no artigo PKI at the crossroads, de autoria de Jennifer Jones, capturado, em <http://www.fcw.com/fcw/articles/2002/0624/tec-pki-06-24-02.asp>, no dia 04.07.2002.

<sup>9</sup> Idem anterior. O texto original diz o seguinte: “*Years in the works, a federal effort to link the public-key infrastructures (PKIs) of agencies has proved quite an undertaking and has been marked by that appears to be rather slow progress*”.

<sup>10</sup> O art. 4º, inciso VII, da MP 2.200-2, determina que compete ao Comitê Gestor da ICP-Brasil “identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais”.

<sup>11</sup> Sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira e a Comissão Técnica Executiva, vide o Decreto nº 3.872, de 18.07.2001. Sobre a necessidade de a COTEC manifestar-se previamente sobre todas as matérias a serem apreciadas pelo Comitê Gestor, vide art. 4º, parágrafo terceiro, inciso I do aludido decreto.

<sup>12</sup> De maneira que foi absorvida e ampliada, pela ICP-Brasil, a iniciativa da ICP-Gov de que tratava o revogado Decreto nº 3.587, de 5.09.2000.

<sup>13</sup> Vide os considerandos da Portaria nº 33, de 08.04.2003.

<sup>14</sup> Esta exigência foi determinada no art. 7º da Medida Provisória nº 2.200-2 e reafirmada no item 3.1.9 da Resolução nº 7.

<sup>15</sup> Vide o parágrafo único do art. 6º da MP 2.200-2 e item 6.1.1 da Resolução nº 7. O não-repúdio é uma presunção relativa de que aquele que assinou digitalmente, a princípio, estará vinculado à declaração de vontade manifestada. Por ser uma presunção relativa ou *juris tantum*, é possível a prova em contrário. Por exemplo, o suposto autor da manifestação de vontade poderá provar que foi coagido a assinar determinado documento eletrônico, e, assim, fazer cessar a presunção de autoria. Todavia, tudo dependerá da análise do conjunto probatório, e se o caso chegar ao Poder Judiciário, o magistrado competente deverá investigar fatos como, se após cessada a coação, o coagido tomou as devidas cautelas para comunicar ao destinatário da mensagem sobre o ocorrido, a fim de paralisar eventual execução contratual (comunicando até mesmo a necessidade de revogação do certificado perante a autoridade certificadora). Enfim, existem infinitas possibilidades de combinação de fatos que deverão ser analisados com prudência e cuidado pelo juiz.

<sup>16</sup> Estes procedimentos estão estabelecidos nos itens 4.4.3 a 4.4.9 (vide também anexo I), da Resolução nº 7.

<sup>17</sup> Como dispõe o item 1.3.4 da Resolução nº 7, que assim continua “(...), que aceitarem certificados de um determinado tipo previsto pela ICP-Brasil, devem aceitar todo e qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitidos por qualquer AC integrante da ICP-Brasil”.

<sup>18</sup> Casos de documentos eletrônicos que tenham de ser arquivados por prazos de tempo ainda maior. Por exemplo, caso os registros de imóveis e os arquivos de registros civis venham a armazenar os seus registros de forma eletrônica, o armazenamento das chaves públicas certamente deverá ser por prazo indeterminado.

<sup>19</sup> Quanto a este aspecto, vide o item 2 do parágrafo quarto do Decreto de Assinatura alemão, de 16.11.2002, o denominado *Signaturverordnung*. Na doutrina alemã, quanto a este aspecto e quanto à valorização e à indispensabilidade do certificado digital fornecido por autoridade certificadora credenciada perante a *Regulierungsbehörde für Telekommunikation und Post*, vide Alexander Roanagel, no artigo **Rechtliche Unterschiede von Signaturverfahren**, publicado na Revista Multimedia und Recht, nº 4, 2002, p. 215-222.

<sup>20</sup> Vide o item 1 do parágrafo quarto da *Signaturverordnung*.

<sup>21</sup> Daí ser de extrema importância o disposto no parágrafo 3º do art. 11 do Projeto de Lei nº 7.316/2002, uma vez que dispõe que, em último caso, a própria AC Raiz, como a âncora de confiança do sistema, acaba por assumir os documentos relativos aos certificados já emitidos por entidade que venha a encerrar as suas atividades.

<sup>22</sup> [www.regtp.de](http://www.regtp.de)

<sup>23</sup> Tradução livre que fiz de trecho do excelente artigo de Ralf Brandner, Ulrich Pordesch, Alexander Roanagel e Joachim Schachermayer, sob o título **Langzeitsicherung Qualifizierter Elektronischer Signaturen** (A proteção duradoura das assinaturas eletrônicas qualificadas), que versa especificamente sobre o tema, publicado na Revista DuD – Datens-chutz und Datensicherheit, nº 2/2002, p. 97-103.



# A privacidade na ICP-Brasil



## Alexandre Rodrigues Atheniense

Advogado. Sócio da Aristóteles Atheniense Advogados S/C. Coordenador do Curso de atualização de Direito na Informática na PUC Minas Virtual. Presidente da Comissão de Informática do Conselho Federal da Ordem dos Advogados do Brasil. Presidente da Comissão de Informática da Seccional de Minas Gerais da Ordem dos Advogados do Brasil. Vice-presidente jurídico da Sucesu-MG.

## RESUMO

O artigo apresenta a delimitação do conceito de privacidade, assim entendido pela doutrina clássica do Direito. Procede-se, então, a uma análise da tutela constitucional da intimidade e da vida privada. Clarifica-se, para fins meramente didáticos, a distinção existente entre os termos "intimidade" e "vida privada". São traçadas algumas linhas a respeito da ideologia da infra-estrutura de chaves públicas, implementada pela Medida Provisória nº 2.200-2, analisando a doutrina nacional a seu respeito. Parte-se, assim, para as críticas a serem feitas em relação à instituição de um certificado único para os usuários e à possibilidade de se realizar análise de tráfego dos certificados revogados pelas autoridades certificadoras.

*Palavra-chave:* privacidade (na ICP-Brasil).

### 1. O conceito do direito à privacidade

O direito à privacidade tem consistido em objeto de estudo de inúmeros juristas ao longo dos anos. No entanto, revela-se, em certa medida, ingrata, a difícil tarefa a que alguns se propunham de delimitar sua abrangência na vida social.

Cumprido esclarecer, portanto, antes de adentrarmos à análise conceitual desse direito, a própria etimologia da palavra, que deriva do termo latino *privatus*, e que,

segundo SAMPAIO (1998)<sup>1</sup>, significa *fora do Estado, pertencente à pessoa ou ao indivíduo mesmo*.

É assim que podemos conceituar a privacidade como uma faculdade inerente a todo e qualquer indivíduo de manter fora do alcance de terceiros o conhecimento sobre fatos inerentes a sua própria pessoa ou atividades particulares.

É o direito à privacidade, destarte, um direito eminentemente subjetivo, delimitado pela própria

cognição do indivíduo. Nesse sentido, assinalou a melhor doutrina norte-americana ao decidir, no caso *Katz vs. United States*, que o direito à privacidade do indivíduo não se estenderia apenas à sua casa e documentos, mas também a qualquer lugar no qual ele pudesse ter *razoável expectativa de privacidade*.

A privacidade concebida em seu sentido lato ainda pode ser entendida como "o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito" (SILVA, 2001)<sup>2</sup>.

O direito à privacidade é, dessa maneira, excepcional, na medida em que consiste num direito negativo, ou seja, expresso exatamente pela não-exposição a conhecimento de terceiro de elementos particulares da esfera reservada do titular (BITTAR, 2001)<sup>3</sup>. Mera espécie do direito à privacidade é o direito à autodeterminação informativa, criação da doutrina espanhola, e comentado por COSTA (2001)<sup>4</sup>:

"Passados pouco mais de 100 anos daquela publicação, vivemos hoje também a necessidade da criação de um novo direito do cidadão, curiosamente nascido daquele direito à privacidade, que acabou consagrado no último século, fundado nas mesmas razões do desenvolvimento tecnológico e de métodos comerciais,

agora por causa da informática e da telemática, e pautado naquela mesma expressão singela, mas marcante, de que nos deixem em paz, direito esse que se constitui na proteção do cidadão em face do tratamento automatizado de seus dados (...).”

No entanto, decerto que a abrangência desse direito não é incondicional. GODOY (2002)<sup>5</sup>, citando CALDAS, nos lembra que: “(...) a vida privada do indivíduo presente, necessariamente, uma face pública, consubstanciada nas contingências da vida de relações, da vida profissional de alguém, de sua obrigatória exposição, (...) essa exposição será maior, a limitar a privacidade, de acordo com a atividade da pessoa (...)”.

Assim é que podemos concluir que o direito à privacidade será tanto menor quanto maior seja a notoriedade ou publicidade do indivíduo, estando certos de que a liberdade de imprensa também é um direito resguardado pela nossa Constituição.

## 2. A proteção constitucional da intimidade e da vida privada

A Constituição Federal consagrou, em seu artigo 5º, inciso X, que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Não obstante, temos a privacidade como valor constitucional inserto no seletor rol de direitos e garantias fundamentais da pessoa humana, sem os quais não se poderia assegurar uma convivência digna e igualitária do tecido social. Nesse particular, vale a

ressalva do art. 60, §4º da Lei Magna que erigiu tal garantia à condição de cláusula pétrea.

Custosa é a distinção doutrinária ao analisar a disparidade entre os termos intimidade e vida privada, inculpidos no rol de garantias individuais de nossa Carta Magna. A doutrina converge, conforme assinala GODOY (2002)<sup>6</sup>, no sentido de que, quando se procura diferenciar vida privada e intimidade do indivíduo, estabelece-se, entre os conceitos, verdadeira relação de gênero e espécie.

E continua, agora citando SERRANO: “(...) privacidade qualificada, na qual se resguarda a vida individual de intromissões da própria vida privada, reconhecendo-se que não só o poder público ou a sociedade podem interferir na vida individual, mas a própria vida em família, por vezes, pode vir a violar um espaço que o titular deseja manter impenetrável mesmo aos mais próximos, que compartilham consigo a vida cotidiana”.

Em que pesem os argumentos de CASTRO (2002)<sup>7</sup> e SZANIAWSKI (1993)<sup>8</sup>, entendemos ser mera dedução lógica o entendimento de que a intimidade consiste em uma vertente do direito à vida privada, estando ambos previstos no bojo da Norma Constitucional em razão de má-técnica legiferante.

De acordo com o *iter* até aqui traçado, resta claro que a privacidade há de ser assegurada independentemente do meio escolhido para a prática de quaisquer atos jurídicos, inclusive o eletrônico, ora objeto desta análise.

Nesse íterim, não podemos entender a privacidade como o direito de estar só, há anos

conclamado pela doutrina anglo-saxônica, mas, sim, como um direito de manter-se, e à sua propriedade, fora do controle de terceiros, o que englobaria, necessariamente, o liame residual competente a cada indivíduo de impedir o acesso e a divulgação de informações sobre sua vida privada.

## 3. O direito à privacidade e sua tutela jurídica

O desenvolvimento de sistemas informáticos tem feito com que a busca pela tutela jurídica efetiva dos direitos da personalidade seja posta em evidência. Assim, podemos notar uma tendência à disciplina desses direitos em alguns códigos modernos, tais quais o italiano (artigos 5 a 10) e o português (artigos 70 a 81).

BITTAR (2001) assinala que *incursões* na vida privada, especialmente ditadas pela evolução da tecnologia e das comunicações, têm exigido o reconhecimento expresso desses direitos e a sua regulamentação, para garantir-lhes proteção no âmbito privado.

No Código Civil Brasileiro de 2002, deixou, o legislador, de tratar do direito à intimidade de forma precisa, limitando-se a estabelecer, em seu artigo 21, que a vida privada é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

A privacidade dos indivíduos é resguardada, portanto, não só em relação a fatos inerentes à sua vida privada, profissional e familiar, mas, também, em relação às suas informações pessoais. Tal qual é a importância dessa proteção, que o Código de Defesa

do Consumidor tutelou, em seu artigo 13, incisos X a XV, algumas condutas consideradas ilícitas em relação à manipulação de informações dos consumidores, quais sejam: impedir ou dificultar o acesso gratuito do consumidor a informações em cadastros, fichas ou registros de dados pessoais (...); elaborar cadastros de consumo com dados irreais ou imprecisos; deixar de comunicar ao consumidor, no prazo de cinco dias, as correções cadastrais por ele solicitadas; etc.

Não obstante a tutela jurídica das informações no âmbito privado, previu, a Constituição Federal, ação mandamental destinada à ciência de informações contidas em bancos de dados pertencentes a entidades públicas ou de caráter público, o *habeas data*.

Assim sendo, em se tratando de entidade ligada à Administração Pública, compete ao indivíduo um instrumento processual adequado como garantia dos direitos previstos no artigo 5º, inciso X (supracitado), XXXIII (direito a receber dos órgãos públicos informações de seu interesse particular) e XXXIV, “b” (obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimentos de situações de interesse pessoal).

Podemos notar, deste modo, que a tutela jurídica da vida privada, dada sua importância, encontra amplo respaldo seja na Constituição Federal, seja em lei infra-constitucional.

#### 4. A infra-estrutura de chaves públicas

O desenvolvimento econômico da internet certamente gera uma demanda para que os negócios

ali realizados sejam acobertados por um certo nível de segurança jurídica. Assim, surge a necessidade tanto da transmissão quanto do conteúdo das informações que trafegam na rede serem conservadas fidedignas para que possam servir de substrato tanto como prova de uma relação ocorrida quanto do convencimento do magistrado em uma eventual lide.

Dessa maneira, insurge-se falar sobre o papel de um terceiro, estranho à relação jurídica e portanto dotado de neutralidade, que detém poderes bastante para autenticar a identidade dos usuários e certificar a autenticidade tanto do conteúdo quanto da transmissão das informações em uma rede, *a priori*, insegura.

Tal qual é a opinião de BARRETO (2001)<sup>10</sup>:

“O papel dos terceiros certificadores insere-se perfeitamente nessa lógica de proporcionar segurança nas transmissões de dados via internet, sem que haja contudo ingerência no conteúdo de tais transmissões, bem como fornecer provas irrefutáveis que possam ser aceitas pelas partes em caso de litígio”.

Esse foi o espírito que motivou a edição da Medida Provisória 2.200-2, de 24 de agosto de 2001, que, dentre outros, instituiu a Infra-estrutura de Chaves Públicas no País.

De imediato, causa-nos estranheza que uma norma de tamanho impacto social seja elaborada por um ato do executivo, o que não deveria ocorrer em uma democracia representativa.

Em que pesem as críticas, instituiu a referida MP, o arcabouço fundamental concernente à vali-

dade jurídica do documento eletrônico. Através deste ato emanado pelo Poder Executivo, adotou-se uma estrutura centralizada – vertical – para a expedição de certificados eletrônicos.

Essa estrutura vertical, por sua vez, foi constituída sob a premissa de que um único certificado digital emitido para o usuário final se prestaria à prática de todos os atos da vida civil, facilitando, assim, a interoperabilidade entre os sistemas de certificação.

Com toda a *venia* às opiniões contrárias, entendemos que a adoção de um certificado único em nada facilitaria a interoperabilidade do sistema por absoluta inexistência de nexo causal entre os fatos.

A simples exigência da observância do credenciamento perante a AC-Raiz, por si só, representaria um risco social e um ônus insuportável a cargo do indivíduo.

A interoperabilidade entre as autoridades certificadoras é relacionada, sim, com o modelo de certificação adotado no mercado, tal como o X.509. BARRETO<sup>11</sup> traz a lume uma interessante ilustração: “Esse modelo é frequentemente referido como o modelo do cartão de crédito, na medida em que reflete o modelo comercial no qual a indústria do cartão de crédito se baseia. Na indústria do cartão de crédito, o que faz o comerciante aceitar o cartão de crédito apresentado pelo consumidor como forma de pagamento é o fato de o cartão ter sido emitido por um banco que ele conhece ou, ainda que o comerciante nunca tenha ouvido falar do banco que emitiu o cartão de crédito, esse banco terá sido certificado por uma companhia de

cartões de crédito (...).

Do momento em que o comerciante conheça e confie na companhia de cartões de crédito, ele poderá confiar no banco e no consumidor, e assim aceitar aquele cartão de crédito como forma de pagamento”.

E continua a referida autora: “A abordagem hierárquica do padrão X.509 oferece algumas vantagens, ao permitir que inúmeros certificados se relacionem a uma mesma raiz confiável”.

Mas o repúdio à estrutura do certificado único não se dá única e exclusivamente em razão de sua interoperabilidade, mas pela ameaça da instituição de um número único para cada indivíduo.

#### 4.1. A adoção do certificado único

A implementação de um certificado único envolveria a congregação de todas as informações acerca do indivíduo em um mesmo suporte, para se compatibilizar à ampla gama de serviços oferecidos no meio eletrônico. Nesse diapasão, assevera SILVA<sup>12</sup> que “o amplo sistema de informações computadorizadas gera um processo de esquadramento das pessoas, que ficam com sua individualidade inteiramente devassada”<sup>2</sup>.

Cumprir lembrar que, no final de 1995, a Comunidade Européia editou a diretiva 95/46 segundo a qual os “Estados Membros devem proteger os direitos e liberdades fundamentais das pessoas naturais, e em particular seu direito à privacidade em relação ao processamento de dados pessoais”.

Além disso, a própria Constitui-

ção Portuguesa vedou expressamente a adoção de um número único exatamente por antever os efeitos que poderiam ser causados pela prática deste ato, *in verbis*:

**“Art. 35.** Utilização da informática:

5 – É proibida a atribuição de um número nacional único aos cidadãos”.

Com efeito, a instituição de um certificado único, como quer implementar e regulamentar o CG – ICPBrasil, acabaria por comprometer a individualidade, intimidade e privacidade do cidadão. Não se pode elidir tal garantia sob a pretensa alegação de facilidade na utilização. Ademais, a instituição de uma AC Raiz (árvore única) garante o monopólio das informações por parte desta instituição, quando o mais seguro seria pulverizar as informações sobre o indivíduo em vários certificados, permitindo-se várias AC Raiz em um sistema floresta. A existência de uma única raiz é justificada pelo fato de permitir a interoperabilidade entre as ACs, entretanto, essa famigerada interoperabilidade pode ser alcançada através da adoção de padrões tecnológicos comuns (v.g. X.509).

A violação de um banco de dados contendo todas as informações pessoais (que será a tônica em um ambiente com certificado único) de um determinado indivíduo representaria um risco social insuportável na medida que sua vida privada poderia ser completa e indevidamente devassada. A utilização de aparatos informáticos facilita o tratamento da informação. Assim, esta violação não atingiria somente o âmbito de relacionamento do in-

divíduo com o órgão em questão, mas todo relacionamento daquele com a sociedade. Bem assevera GRECO (2000)<sup>13</sup> ao afirmar que: “numa sociedade complexa (...) o poder advém da posse de informações sobre pessoas, eventos ou coisas”<sup>3</sup>.”

A existência destes vários cadastros é, na verdade, uma garantia de que o indivíduo não terá sua vida devassada na medida em que dificulta o cruzamento de tantas informações complexas. Essa é a principal razão pela qual a instituição de um certificado único foi rechaçada pelos países europeus.

#### 4.2. A análise de tráfego

Outra questão controvertida em relação a ICP-Brasil concerne à análise de tráfego da consulta dos certificados revogados. Na utilização de um certificado digital, a verificação da lista de certificados revogados, mantida pela autoridade certificadora, poderia gerar, para diversos fins, um *log*, que em última análise pode fornecer algumas informações sobre aquele usuário.

Apesar de não ser capaz de acessar o conteúdo da mensagem em razão da certificação digital, o simples fato de ter ciência da comunicação seria capaz de ameaçar a privacidade dos usuários, uma vez que muitas informações podem ser obtidas através da análise do perfil (intervalo de tempo, tamanho, datas e horários das mensagens) dessas mensagens. A violação da privacidade do indivíduo poderia dar-se não pelo conhecimento do conteúdo que foi transmitido, mas de uma forma muito mais sutil, através do conhecimento da existência de comunicação



entre as partes. Afirma o professor SCHNEIER<sup>14</sup> que “often the patterns of communication are just as important as the contents of communi-

cation”<sup>4</sup>. Diante dessas considerações, reiteramos a crítica no sentido de não privilegiar o avanço tecnológico em detrimento dos direitos

e garantias fundamentais. E, ainda, compatibilizar a regulamentação da ICP Brasil com a ideologia constitucionalmente adotada.

---

## Notas

<sup>1</sup>. SAMPAIO, José Adércio Leite, *Direito a Intimidade e à Vida Privada*, Belo Horizonte: Del Rey, 1998, p.34

<sup>2</sup>. SILVA, José Afonso da Silva, *Curso de Direito Constitucional Positivo*, 19ª ed., São Paulo: Malheiros, 1997, p.209

<sup>3</sup>. BITTAR, Carlos Alberto, *Os Direitos da Personalidade*, 5ª ed. rev., atual., ampl. por Carlos Bianca Bittar. Rio de Janeiro: Forense, 2001, p. xx, p. xx, p. 108

<sup>4</sup>. COSTA, Marcos da, *Novos Ventos Digitais*, disponível em: [http://www.marcosdacosta.adv.br/documento.asp?ID\\_Documento=455](http://www.marcosdacosta.adv.br/documento.asp?ID_Documento=455) - acesso em: 15/05/2003

<sup>5</sup>. GODOY, Cláudio Luiz Bueno de, *A Liberdade de Imprensa e os Direitos da Personalidade*. São Paulo: Atlas, 2001, p.47;

<sup>6</sup>. Op. Cit. 5, p. 49

<sup>7</sup>. CASTRO, Mônica Neves Aguiar da Silva, Honra, *Imagem, Vida Privada e Intimidade em Colisão com Outros Direitos*. Biblioteca de Teses. Rio de Janeiro: Renovar, 2002, p.32

<sup>8</sup>. SZANIAWSKI, Elimar, *Direitos da Personalidade e sua Tutela*. São Paulo: RT, 1993, p. 132

<sup>9</sup>. Op. Cit. 3, p.35

<sup>10</sup>. BARRETO, Ana Carolina, *Assinaturas Eletrônicas e Certificação*, In: ROCHA FILHO, Valdir de Oliveira (coord.), *O Direito e a Internet*, Rio de Janeiro: Forense Universitária, 2002, p.44

<sup>11</sup>. Op. Cit. 10, p.48

<sup>12</sup>. Op. Cit. 2, p.212

<sup>13</sup>. GRECO, Marco Aurélio, *Internet e Direito*, 2ª ed., rev. e aum., São Paulo: Dialética, 2000, p.194

<sup>14</sup>. SCHNEIER, Bruce, *Secrets & Lies Digital Security in a Networked World*, Wilye Computer Publishing, 2000, p.34

---



# Tudo que você deve saber sobre certificação digital



## Jeroen van de Graaf

Pesquisador em criptografia há mais de 20 anos e doutor na área pela Universidade de Montreal, Canadá. Atualmente, trabalha como pesquisador na UFMG e atua como consultor autônomo através da sua empresa, a VDG-InfoSec.

## RESUMO

No mundo convencional de papel, estamos acostumados às propriedades de autenticidade, integridade e não-repúdio de documentos que, juntas, criam a fé indispensável para quase todos os processos burocráticos. Para um mundo digital (sem papel) dar certo, é necessário que essas propriedades continuem valendo. Este texto tenta explicar as noções básicas das novas tecnologias que estão surgindo para garantir a fé de documentos no mundo digital: a assinatura digital, o certificado digital e a infra-estrutura de chaves públicas, entre outros.

O texto tenta simplificar o máximo possível. No entanto, também não é desejável simplificar demais esse assunto complexo e fascinante; senão há o risco de perder a essência e enganar o leitor. Espero que minha tentativa contribua para a compreensão desse assunto por um público maior.

### 1. Assinar um documento convencional

Todo mundo já assinou um documento. A única observação importante é que cada assinatura é igual (em teoria), e que a ligação entre o texto do documento e a assinatura é o meio físico subjacente: o papel.

### 2. Assinar um documento digital

Uma assinatura digital é o resul-

tado de uma computação que tem duas entradas: um documento eletrônico e uma chave criptográfica e secreta. A computação embaralha todos os bits do documento e da chave, resultando numa seqüência de bits de tamanho fixo (normalmente 1024 bits). Esta é a assinatura digital, que é anexada ao documento original.

Uma assinatura digital tem a seguinte característica: sem acesso à chave secreta, é matematicamente impossível calcular qual a

seqüência de bits que constitui a assinatura digital. Claro, um forjador sempre pode “chutar” uma assinatura. Mas a probabilidade de acertar corresponde a ganhar a MegaSena 40 vezes seguidas, um evento tão improvável que, na prática, pode ser mesmo desconsiderado.

Observe que a autenticidade e o não-repúdio do documento assinado digitalmente se baseiam no conhecimento da chave: quem é dono da chave secreta é autor daquele documento. Portanto, o sigilo da chave é de suma importância. A integridade do documento se baseia numa outra característica do método da computação: se um bit do documento original for mudado, a assinatura sai completamente diferente; então, adulterar um documento assinado é impossível.

A assinatura digital se parece muito com a assinatura de punho, ou com o selo do mundo tradicional de papel. No primeiro exemplo, a chave secreta corresponde aos movimentos motores do assinante e, no segundo, é supostamente impossível recriar (ou seja, forjar) o selo, com sua estrutura fina de linhas, papel e tinta especial, etc. Como no mundo digital não há meio físico, a assinatura depende não apenas da chave, mas também do documento. Obviamente, deve ser assim; senão seria muito fácil cor-

tar uma assinatura digital de um documento e colá-la embaixo de um outro.

### 3. Verificar uma assinatura convencional

Até agora, falamos apenas sobre como assinar documentos, mas igualmente importante é como se verifica uma assinatura. Para entender mais tarde a verificação no mundo digital, é importante lembrar como isso funciona no mundo tradicional. São procedimentos tão cotidianos que é fácil se esquecer da sua importância. Para assinaturas de punho, é comum que um indivíduo se dirija pessoalmente a uma “autoridade” (um banco, um cartório). A autoridade confere a identidade da pessoa e cria uma ficha com dados pessoais e outros dados relevantes, e com a assinatura daquela pessoa. Em princípio, depois dessa visita, o indivíduo nunca mais precisa voltar. Quando um terceiro mostrar à autoridade um documento supostamente assinado por aquele indivíduo, ela procura a ficha, compara as duas imagens das assinaturas e dá um veredicto: a assinatura é válida ou não. Com selos, a situação é um pouco diferente, eles são emitidos por órgãos que já têm autonomia, então, não precisam de uma autoridade. Mas, nesse caso, também devem existir modelos para que terceiros possam comparar.

### 4. Verificar uma assinatura digital

No mundo digital, a verificação de uma assinatura é muito parecida, e em alguns pontos até mais flexível. Dada a chave secreta que é usada para assinar, é possível criar uma outra chave pública correspondente, que é usada na ve-

rificação da assinatura. Esse par de chaves tem uma característica surpreendente: mesmo conhecendo a chave pública, é matematicamente impossível calcular a chave secreta correspondente. Este modelo é conhecido como criptografia com chaves públicas. É diferente da criptografia convencional descrita nos livros de espionagem: neles, a chave para cifrar e decifrar deve ser a mesma, e ela não pode ser pública.

No mundo convencional, a chave secreta (também chamada de chave privada) corresponde aos movimentos motores do indivíduo, enquanto a chave pública corresponde à imagem da assinatura no papel, um dado que é público. E como no mundo convencional é necessário vincular a imagem da assinatura a uma identidade, é necessário que exista o mesmo procedimento no mundo digital. O indivíduo se dirige a uma autoridade com a sua chave pública (e talvez com outros documentos comprovando sua identidade), a autoridade confere a identidade da pessoa e cria uma ficha com os dados pessoais e a chave pública daquela pessoa.

Mas, em vez de guardar essa ficha no seu arquivo, a autoridade assina-a e publica-a na internet! É esse documento, contendo uma chave pública e os dados pessoais do seu dono, que é chamado um certificado digital. Ou seja, o certificado digital corresponde à ficha do cartório, carimbada pelo tabelião, publicada livremente. Um certificado digital não é sigiloso; ao contrário, pode e deve ser copiado e distribuído à vontade. A grande vantagem é que qualquer pessoa, em qualquer lugar no mundo com acesso à internet, pode verificar a assinatura.

Em outras palavras, verificar uma assinatura digital é parecido com verificar uma assinatura convencional: têm-se o documento assinado e o certificado digital; o último contém a identidade do assinante e a sua chave pública. E, através de uma segunda computação matemática, verifica-se se os dois conferem, ou seja, se a chave secreta usada para assinar o documento corresponde à chave pública no certificado.

### 5. Infra-estrutura de Chaves Públicas (ICP)

Note bem como funciona a cadeia de confiança no exemplo anterior: a identidade do assinante é garantida pela autoridade que emitiu (assinou) o certificado digital, comumente chamada Autoridade Certificadora (AC). Ou seja, é necessário que o verificador conheça a chave pública daquela AC para verificar se o certificado foi realmente assinado por ela. É nesse ponto que as coisas se complicam.

Como existem milhares de bancos e cartórios geograficamente espalhados no Brasil e no mundo, é claro que devem existir milhares de ACs. Mas é inviável que um verificador conheça todas as chaves públicas dessas autoridades. Portanto, por motivos de escalabilidade, existem “meta-autoridades”, que credenciam autoridades intermediárias, que emitem certificados a indivíduos.

O resultado é uma hierarquia de autoridades certificadoras: existe apenas uma AC-Raiz cujo único papel é emitir certificados para suas AC-intermediárias. Elas, por sua vez, emitem certificados para os indivíduos ou entidades pertencentes à hierarquia. Um sentido do termo Infra-estrutura de Chaves Públicas (ICP) é essa hierar-



quia (ou árvore) de certificação. Por exemplo, na ICP-Brasil há uma AC-Raiz e seis ACs-Intermediárias de primeiro nível: a Presidência da República, a Serasa, a Receita Federal, o Serpro, a Caixa Econômica Federal e a CertiSign.

Aliás, existe um outro uso da sigla ICP (PKI=Public Key Infrastructure, em inglês), o que cria bastante confusão. Como deve ser óbvio, existe uma quantidade enorme de padrões, software, hardware, procedimentos e documentos para essa tecnologia funcionar. O termo Infra-estrutura de Chaves Públicas (ICP), no sentido amplo, é usado também para se referir a esse conjunto, à tecnologia em geral.

Felizmente, existe um padrão adotado mundialmente (PKIX-X.509) e existe software livre para construir uma ICP (hierarquia). Por exemplo, o meu notebook contém um software para criar uma ICP funcional. No entanto, esse programa só serve para pesquisa, não é uma solução viável para gerenciar uma ICP com centenas de certificados. Mesmo assim, há uma implicação importante aqui: qualquer pessoa pode criar uma ICP. A padaria na esquina, o Minas Tênis Clube, a UFMG, o Estado de Minas Gerais, todo mundo pode emitir certificados. Então, se não houver impedimentos técnicos para emitir certificados, qual é a credibilidade (o valor) de um certificado?

## 6. A credibilidade de certificados

Nesse contexto, uma outra comparação com o mundo tradicional é muito interessante. Nossa carteira é cheia de documentos

que atestam nossas credenciais: carteira de identidade, carteira de motorista, cartões de crédito, carteirinha da biblioteca da UFMG, carteirinha da videolocadora, carteirinha de seguro de saúde, etc., etc. A credibilidade dessas não depende do documento em si, mas da política de quem o emitiu. Por exemplo, a credibilidade de um cartão American Express Platinum é diferente da do cartão Carrefour. E a carteira de identidade tem uma grande credibilidade para terceiros, porque todo mundo sabe que há um processo rigoroso por trás para consegui-la, enquanto a carteirinha da videolocadora não tem validade nenhuma porque todo mundo consegue facilmente.

Com certificados digitais é igual: a sua credibilidade depende completamente da política adotada pela autoridade certificadora emissora. Por exemplo, existe um site na internet que emite certificados automaticamente, sem verificação nenhuma e, portanto, sem credibilidade nenhuma, mas mesmo assim é útil para testes. Existem empresas que emitem um certificado a qualquer cidadão com nome, CPF e título de eleitor, após a verificação desses dados, cobrando uma taxa de 100 reais anual. E para ser AC-intermediária subordinada à AC-Raiz da ICP-Brasil é necessário pagar centenas de milhares de reais como taxa (sem falar dos custos para montar uma sala-cofre, que custa milhões, para guardar a chave privada). Lembre-se que, em todos os casos, estamos falando de certificados que são simplesmente bits, nem possuem um holograma bonito. Repito, a credibilidade do certificado advém da credibilidade da AC. Aliás, introduzindo carteiras de

identidade, mudamos sutilmente de assunto. Em vez de discutir a assinatura digital, que provê autenticidade, integridade e não-repúdio de documentos, estamos discutindo identificação: como estabelecer a identidade de pessoas. E, em muitas situações, ela é importante, porque associada a ela estão privilégios e direitos, por exemplo, o direito de dirigir um carro. Ou seja, a identificação leva a uma autorização. A tecnologia ICP serve também para implementar a identificação e autorização das pessoas no mundo digital.

Ainda por cima, a mesma tecnologia também pode ser aplicada para proteger o sigilo de documentos e comunicações, mas, na maioria das situações, as organizações não se preocupam com o sigilo, e, sim, com a fé dos documentos e processos, ou seja, com as questões de autenticidade, integridade e não-repúdio de documentos, e identificação de pessoas.

## 7. O lado comercial da certificação digital

O valor econômico dessa tecnologia foi logo percebido nos anos oitenta, mas explodiu com a chegada da internet. Em particular, o certificado digital é um mecanismo poderoso para estabelecer uma identidade digital das pessoas. Como explicamos, ele serve para assinar documentos, e também para comprovar a identidade. As maioria das empresas que atua nessa área ganha dinheiro cobrando pela emissão de certificados. As empresas colocam um prazo de validade de um ano, normalmente, garantindo uma fonte de renda regular. Na realidade, muitas vezes elas deixam de explicar a seus clientes

que criar uma própria ICP poderia ser uma opção interessante, dependendo das circunstâncias.

## 8. A ICP-Brasil

A ICP-Brasil foi uma iniciativa do governo anterior com a intenção de unificar a certificação digital no Brasil. Ela passa a impressão de que deve existir uma única ICP no Brasil, com ela ao topo. A própria palavra “infra-estrutura” pode levar o leigo a crer nisto, inconscientemente fazendo a analogia com a rede elétrica num país. Porém, a analogia certa é com a telefonia celular: podem existir vários operadores de telefonia celular paralelamente.

Não é sempre preciso aderir à ICP-Brasil para usar a certificação digital, às vezes nem é aconselhável. Primeiro, se uma organização (pública ou privada) quer emitir certificados para uso interno, ela obviamente tem o direito de fazê-lo. Qual é o ganho de aderir à ICP-Brasil, cujas exigências de segurança são rígidas demais para muitas organizações, e cujas taxas são altas? Segundo, há a questão de autonomia: várias organizações não querem ou não podem se subordinar a um órgão do Poder Executivo Federal.

E terceiro, a Medida Provisória 2200-2, que criou a ICP-Brasil, inclui um parágrafo (10.2) dizendo que se duas partes concordarem em assinar documentos usando certificados emitidos por uma ICP que não pertence à ICP-Brasil, estes documentos têm valor jurídico.

Ou seja, para uso interno, ou para partes que entram em acordo, não há necessidade de usar a ICP-Brasil.

## 9. ICPs alternativas

Por estes motivos, e por motivos de pesquisa e educação, as universidades brasileiras, lideradas pela UFSC, a Unicamp e a UFMG, estão criando uma ICP independente. Através de um projeto da Rede Nacional de Desenvolvimento e Pesquisa (órgão de pesquisa do MEC e MCT), elas criaram em 2005 a ICP-EDU, uma ICP no âmbito acadêmico, baseada em software livre. A OAB já criou sua própria ICP.

Então, é provável que coexistirão várias ICPs; isto é inevitável. Pela mesma razão que todos nós temos uma grande variedade de carteiras, carteirinhas e cartões, refletindo nossas relações diversas com entidades públicas e privadas, teremos vários certificados diferentes emitidos por ICPs diferentes. Se isso levar a confusão, uma solução seria padronizar as políticas das ICPs por lei, não a imposição de uma única ICP.

## 10. A questão da privacidade

Pessoalmente, não acredito que a idéia de unificar todos esses certificados em um único, emitido pela ICP-Brasil, vá dar certo, porque combinar todos as funcionalidades requeridas por vários órgãos públicos é muito complicado.

Aliás, seria o grande sonho do Grande Irmão, um certificado único por cidadão: pode-se rastrear a vida digital de uma pessoa completamente. Essa questão da privacidade fez vários países desistirem de uma ICP nacional, mas no Brasil ninguém se parece preocupado; ainda não vi nenhuma proposta lidando adequadamente com esta questão.

## 11. Conclusão

Certificação digital é uma tecnologia muito promissora, pois ela permite implementar o não-repúdio e a identificação de pessoas jurídicas e físicas no mundo digital. Mas é uma tecnologia nova, e ainda há bastantes questões tecnológicas, econômicas, jurídicas e políticas a serem resolvidas.

Porém, o maior obstáculo é cultural: estamos todos apegados ao mundo do papel. Uma prova disso é que a primeira imagem que entra em nossa mente quando pensamos na palavra “documento” é a do papel, e não as informações escritas nele. Ou seja, o mundo digital traz uma separação de mídia e conteúdo que no mundo de papel não existia. Ainda mais forte: no caso de uma assinatura de punho, a ligação entre o conteúdo e a assinatura é estabelecida através da mídia; o papel é apenas intermediador, porém essencial na questão da autenticidade e, portanto, da validade jurídica.

Até que todo mundo se acostume ao documento eletrônico e confie na sua autenticidade, vai levar muitos anos, talvez décadas. É uma profunda mudança de paradigma.

# Certificação Digital - Uma Realidade em Minas



## Raymundo Albino

Engenheiro eletricista e analista de suporte de sistemas, graduado pela PUC-MG. Atua como assessor técnico da Diretoria de Tecnologia e Produção da Prodemge, tendo passado pela Gerência de Redes e Superintendência de Produção. Participa atualmente do grupo de trabalho criado pelo governador para implantar a certificação digital no âmbito do Estado de Minas Gerais.



## Sérgio Daher

Engenheiro eletricista e analista de suporte de sistemas, graduado pela PUC-MG. Atua como superintendente de Tecnologia e Suporte da Prodemge, já tendo exercido diversos cargos gerenciais na empresa. Participa do Grupo de Trabalho de Certificação Digital, instituído pelo Governo do Estado de Minas Gerais.

## RESUMO

O artigo dá uma visão global da necessidade do uso da certificação digital nas instituições, tanto públicas como privadas, especialmente devido ao uso crescente da internet em transações e relacionamentos entre empresas e cidadãos, buscando sempre garantir a Confidencialidade, Integridade e Disponibilidade das informações.

Em seguida, é feita uma explicação sobre conceitos de criptografia, assinatura digital e certificação digital, mostrando as principais aplicações já em uso no Brasil.

O artigo é concluído com a posição da certificação digital no Estado de Minas Gerais, mostrando o que já foi feito e as aplicações já eleitas para utilizarem os benefícios desta tecnologia nos órgãos e entidades estaduais, visando à agilização da máquina administrativa e à melhoria dos processos de relacionamento entre o Estado e o cidadão.

**Palavras-chave:** Certificação Digital (do Estado de Minas Gerais)

Com o crescente aumento de utilização da internet para o trâmite de documentos eletrônicos, verifica-se que as organizações, tanto públicas como privadas, estão cada vez mais preocupadas com a segurança e legalidade desses processos. Quanto à segurança no tráfego

e armazenamento de documentos eletrônicos, os aspectos que mais preocupam as organizações são: sigilo, integridade, autenticidade e não-repúdio. Quanto à legalidade, as preocupações se voltam para a validade jurídica e força probatória. Informações sigilosas são aque-

las que só podem ser acessadas pelo legítimo receptor do documento. A integridade é a garantia de que o documento recebido não está alterado ou fraudado. A autenticidade é a garantia de autoria do emissor ou aprovador do documento. O não-repúdio é a impossibilidade do emissor negar a realização da transação ou autoria. Quanto à legalidade, um documento ou processo eletrônico terá validade jurídica quando aceito como prova e força probatória e quando não puder ser impugnado em uma eventual contestação.

Hoje, a certificação digital, combinando aspectos tecnológicos e jurídicos, possibilita tratar a segurança e legalidade de documentos e processos eletrônicos com garantia de autenticidade, integridade, sigilo, não-repúdio e legalidade. Cresce a cada dia o número de empresas e organizações governamentais que, descobrindo as potencialidades da certificação digital, passam a implementar soluções baseadas nessa tecnologia, aumentando a segurança de seus processos.

## Criptografia

A inviolabilidade de informações sensíveis é uma preocupação constante da humanidade já há muitos séculos. Inúmeros mecanismos de codificação de informações foram

utilizados, com objetivo de reduzir a possibilidade de que adversários obtivessem informações secretas, através da captura de documentos em trânsito ou arquivados.

Historicamente, temos evidências da utilização de mecanismos criptográficos remontando à China antiga. Como exemplo, mostraremos a CIFRA DE CÉSAR, um pouco mais moderna, da época em que Júlio César governava o Império Romano. Este método foi concebido através da substituição posicional do alfabeto, utilizando uma chave que marca o deslocamento a ser adotado na codificação da mensagem. A seguir, mostramos um exemplo onde é utilizada a chave 6, ou seja, cada letra do alfabeto da mensagem original deverá ser substituída pela letra que estiver na 6ª posição anterior, para formar a mensagem cifrada:

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**  
**U V W X Y Z A B C D E F G H I J K L M N O P Q R S T**

**CHAVE = 6**

**ORIGINAL SIGILO PELA CRIPTOGRAFIA**  
**CIFRADA MGACF IUJZ FVUXLCJNIALV CV**

Junto ao desenvolvimento da humanidade, métodos cada vez mais sofisticados foram desenvolvidos, sempre na disputa de uma verdadeira guerra: métodos mais sofisticados de cifragem contra métodos cada vez mais aperfeiçoados de decifragem.

O desenvolvimento da informática tem sido um grande aliado na guerra da criptografia, permitindo que sistemas extremamen-

te complexos de codificação possam ser desenvolvidos, assim como mecanismos de decodificação, também superpoderosos, possam ser concebidos e implementados.

O objetivo é alcançar condições onde mesmo os mais poderosos computadores tenham chances mínimas de decifragem de mensagens em prazos em que métodos administrativos de segurança possam ser implementados a custos razoáveis (troca sistemática de chaves).

O método mais eficaz conhecido é o modelo de chave pública utilizando exponenciação. Cada participante da estrutura possui uma chave secreta e uma chave pública. Assim sendo, uma mensagem, para ser enviada, é inicialmente criptografada pela chave do receptor, garantindo que só ele seja capaz de decifrar a mensagem

através de sua chave secreta. Este processo, utilizando uma chave de duzentos algarismos, dependeria 10 milhões de séculos de um computador capaz de 1 milhão de multiplicações por segundo para que o sigilo fosse quebrado.

O método pode também ser utilizado em sistemas de assinatura eletrônica, quando, então, um documento poderá ser enviado

eletronicamente com garantia de origem e destino.

Apesar da transcrição anterior ser datada de 1992, quando foi publicada na revista comemorativa dos 25 anos da Prodemge, época ainda anterior à realidade atual do mundo Web, demonstra-se atual nas técnicas da segurança da informação.

O que ocorreu nos anos que se seguiram foi a massificação da sua utilização através das aplicações de comércio eletrônico, hoje utilizado por toda a comunidade conectada à internet, seja para a compra de mercadorias e serviços, ou mesmo a consulta do saldo de uma conta corrente bancária através da Web.

O estágio atual da utilização das técnicas de criptografia no ambiente das transações eletrônicas se resume, na grande maioria das aplicações, à garantia da autenticidade do destino a que se conecta o usuário, assegurando-lhe que a instituição, na qual uma determinada transação está sendo efetuada, seja aquela que ele realmente deseja e espera, preservando também o sigilo das comunicações trocadas durante o procedimento.

O que nos avizinha é a identificação inequívoca também do usuário dos sistemas de informação, obtida através de certificados digitais pessoais, seja de pessoas físicas ou jurídicas, garantindo, desta forma, a impossibilidade do repúdio da realização das transações por elas originadas.

Tal realidade, em um futuro próximo, trará garantias adicionais a toda a comunidade envolvida com o mundo das transações eletrônicas, destino inexorável de toda a civilização.



# Sistema de Criptografia RSA

## O receptor da mensagem:

- > escolhe dois números primos,  $p$  e  $q$ , calculando  $n=p \cdot q$ ;
- > determina  $\phi(n) = (p-1) \cdot (q-1)$ ;
- > escolhe o expoente de codificação, tal que  $1 < e < \phi(n)$  e  $\text{mdc}(e, \phi(n)) = 1$ ;
- > determina o expoente de decodificação, tal que  $1 < d < \phi(n)$  e  $ed = 1 \pmod{\phi(n)}$ ;
- > publica o par  $(n, e)$ , que se diz a Chave Pública, mantendo secreto o par  $(n, d)$ , a Chave Privada.

## O emissor da mensagem:

- > converte a mensagem no número inteiro  $M$ ,  $0 < M < n$ , recorrendo a um "alfabeto digital", por exemplo,  $A = 01$ ,  $B = 02$ ,  $C = 03$ , ...,  $Z = 26$ ;
- > obtém a chave pública  $(n, e)$  do destinatário;
- > converte o número  $M$  no número  $C$  através da fórmula de codificação:  
 $C = M^e \pmod{n}$ , onde  $M$  representa a mensagem original e  $C$  a mensagem codificada;
- > envia a mensagem  $C$ , ao destinatário.

## O receptor da mensagem:

- > determina o inteiro  $M'$  usando a fórmula de decodificação  $M' = C^d \pmod{n}$ ;
- > como  $M' = M$ , recorre ao "alfabeto digital" e obtém a mensagem original.

## Exemplo:

### Determinação das chaves

- > Primos  $p=11$  e  $q = 23$ ;  $n = 11 \times 23 = 253$ , e  $\phi(n) = (11 - 1)(23 - 1) = 10 \times 22 = 220$ .
- > Como  $\text{m.d.c.}(3, 220) = 1$ , o expoente de codificação é  $e = 3$ .
- > Como  $3d = 1 \pmod{220}$  -  $d = 147$ , o expoente de codificação é  $d = 147$ . Assim, a chave pública é  $(253, 3)$  e a chave privada é  $(253, 147)$ .

### Codificação da mensagem SOL

- > Recorrer-se a um "alfabeto digital":  $M = 191512$ .
- > Como  $M > n = 253$ , divide-se  $M$  em blocos  $M_1 = 19$ ,  $M_2 = 15$  e  $M_3 = 12$ .
- > Usando a chave pública  $(253)$ , efetua-se a codificação de cada um dos blocos:  $19^3 = 6859 = 28 \pmod{253}$ ,  $15^3 = 3375 = 86 \pmod{253}$  e  $12^3 = 1728 = 210 \pmod{253}$
- > A mensagem codificada é  $C = 2886210$ .

### Decodificação da mensagem

- > Usando a chave privada,  $(253, 147)$ , tem-se:  $28147 = 19 \pmod{253}$ ,  $86147 = 15 \pmod{253}$  e  $210147 = 12 \pmod{253}$
- > Portanto,  $M' = 191512 = M$
- > Conhecido o número  $M$ , basta recorrer ao "alfabeto digital" para obtermos a mensagem inicial: SOL.

## Assinatura Digital

Logicamente, nos dias de hoje, cifras tão simples como a Cifra de César, e até mesmo aquelas mais complexas utilizadas antigamente, seriam facilmente quebradas pelo uso de computadores, através de um método denominado "força-bruta", onde são realizadas tentativas sucessivas até se chegar à chave desejada.

A criptografia moderna, essencial para a segurança de computadores conectados em rede, especialmente à internet, consiste em algoritmos complexos, de forma a dificultar ao máximo a ação de invasores.

As funções de criptografia aplica-

das aos computadores podem ser divididas em duas categorias: *criptografia* e *autenticação*.

## Criptografia

O ato de criptografar, conforme já abordado e detalhado a seguir, se refere ao embaralhamento das informações de uma mensagem, de forma que alguém sem autorização não possa compreendê-la.

## Autenticação

Já a autenticação é o procedimento para verificação de autenticidade do emissor da mensagem. Para realizar uma autenticação, é necessário proteger a mensagem de forma que ela não

seja modificada, o que é normalmente feito através da incorporação de uma *assinatura digital*.

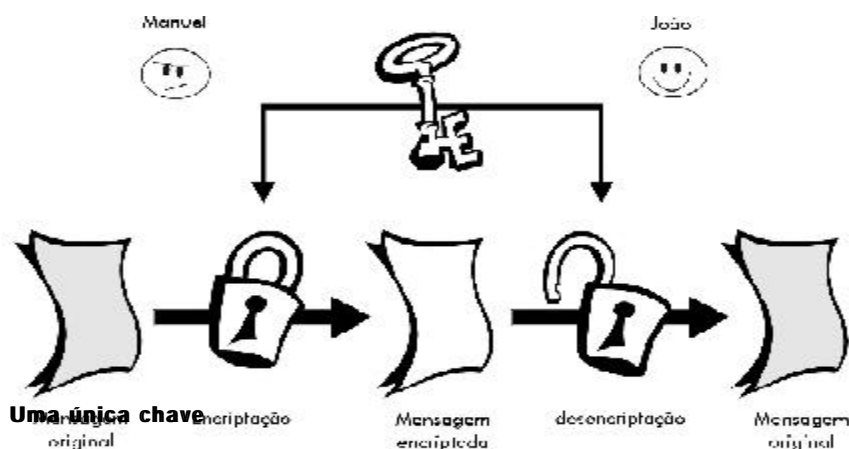
Tipicamente, uma assinatura é formada pela utilização de uma função denominada *hash*, que consiste no cálculo e codificação de um resumo da mensagem completa, formando um código de tamanho fixo que é cifrado e transmitido junto com a mensagem original, garantindo a autenticidade da mensagem.

Podemos dividir as técnicas de criptografia em dois tipos básicos: Criptografia Simétrica ou de Chave Privada, onde uma única chave é utilizada para criptografar e decifrar, e Criptografia Assimétrica ou de Chave Pública, onde é usado um par de chaves

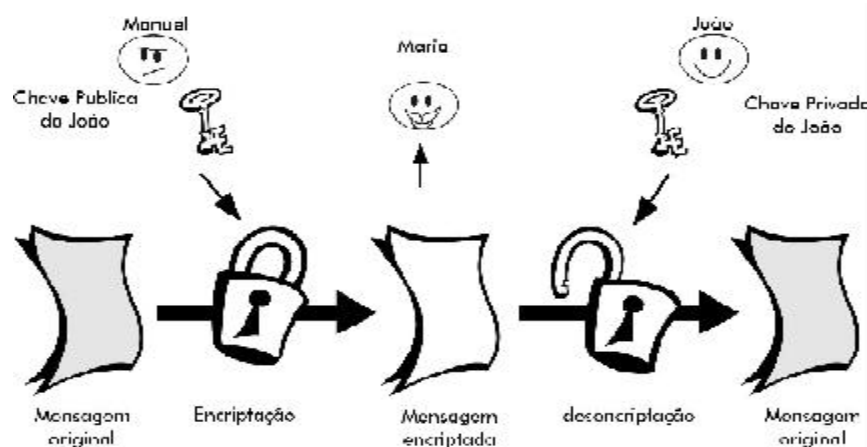
relacionadas entre si, que são a chave pública e a chave privada. As técnicas de criptografia simétricas mais conhecidas são a DES e a AES. O RSA é o algoritmo assimétrico mais conhecido.

## Tipos de Criptografia

### \* Criptografia Assimétrica ou de Chave Pública



### \* Criptografia Simétrica ou de chave secreta



**Duas chaves:** - chave pública, que é publicada;  
- chave privada, que é mantida secreta.

No âmbito da certificação digital, a modalidade mais utilizada é a denominada híbrida, como o protocolo SSL, que utiliza a criptografia assimétrica na inicialização de uma sessão Web, quando é trocada uma chave simétrica, tipo DES, que será utilizada no transcorrer da sessão já iniciada, até o seu término, quando então é descartada.

Tal procedimento visa a alcançar o máximo de segurança - porque a chave simétrica é utilizada apenas uma vez, sendo que ela é gerada dinamicamente, a cada sessão estabelecida - aliado ao mínimo de processamento necessário nos computadores envolvidos. Assim, o algoritmo DES consome menos recursos computacionais quando comparado ao algoritmo RSA utilizado na criptografia assimétrica, ou de chave pública.

Para realizar a assinatura de documentos, é necessária a utilização de um par de chaves, sendo que o emissor assina o documento com sua

chave privada, e o receptor deverá possuir a chave pública do emissor para que possa ser comprovada a autenticidade do documento.

Já no caso de emissão de documento sigiloso criptografado, o procedimento é o oposto, ou seja, o emissor deverá possuir a chave pública do receptor, de forma que somente ele, ao receber o documento, poderá decifrá-lo com a sua chave privada.

No caso de documentos assinados e criptografados, deverão ser seguidos os dois procedimentos anteriormente citados em conjunto.

É importante salientar a diferença entre assinatura digital (explicada acima) e assinatura eletrônica, que pode ser, por exemplo, um e-mail transmitido em claro, o qual não possui garantia de autenticidade.

A geração de um par de chaves está demonstrada no quadro da página ao lado.

## Certificação Digital

A certificação digital é o procedimento que utiliza um arquivo eletrônico que acompanha um documento assinado de forma digital, cujo conteúdo é criptografado. Este documento é denominado *certificado digital* e contém informações que identificam a pessoa e/ou computador com que se está tratando na rede. Um documento eletrônico que possui certificação digital tem garantia de autenticidade de origem e autoria, de integridade de conteúdo, de confidencialidade e de não-repúdio, ou seja, de que a transação, depois de efetuada, não poderá ser negada pela parte que

utilizou a certificação.

O certificado digital é uma credencial eletrônica definida de acordo com o padrão ITU-T X.509, e é emitido por uma Autoridade Certificadora (terceiro de confiança) que garante a identidade do portador / usuário de forma análoga a uma Carteira de Identidade.

A Autoridade Certificadora - AC- e a Autoridade de Registro - AR- são entidades de confiança responsáveis pela emissão dos certificados, bem como pela manutenção de toda a estrutura vinculada à certificação digital dentro de seu âmbito de atuação. Dentro da ICP-Brasil, as ACs e ARs estão credenciadas em uma estrutura hierárquica, que tem uma *Chave Raiz* responsável pela geração das Chaves Secundárias, que por sua vez emitem os certificados de usuários.

As aplicações de certificação digital podem ser divididas em duas categorias que são a certificação pessoal e a certificação de servidores.

#### > Certificação Pessoal

- A certificação pessoal refere-se aos certificados emitidos em nome de uma pessoa natural ou jurídica, de forma a identificá-la inequivocamente, ou seja, a pessoa, ou o representante legal da entidade, associada àquela pessoa jurídica.

Tais certificados são utilizados na assinatura de mensagens eletrônicas, bem como no relacionamento dessas pessoas com os aplicativos que exigem a identificação segura de seus usuários.

#### > Certificação de Servidores

- A certificação de servidores se destina à identificação de serviços ou grupos de serviços associados a uma determinada URL primária, Uniform Resource Locator, que é o identificador mundial de documentos e demais recursos na internet, ou seja, todas as URLs derivadas de um determinado endereço eletrônico de um servidor.

Este mecanismo garante que as informações obtidas se originam verdadeiramente daquele endereço certificado, a exemplo dos bancos e demais aplicações que requerem segurança da informação.

São exemplos bem-sucedidos de utilização de certificação digital no Brasil:

- o e-CPF e o e-CNPJ na Secretaria da Receita Federal, que possibilitam o relacionamento seguro via internet dos contribuintes com a instituição para acesso de informações não disponíveis de forma convencional;

- o processo de tramitação eletrônica de documentos oficiais, que serão publicados no Diário Oficial da União, utilizado pelo Presidente e seus ministros, que possui um sistema que faz o controle do fluxo de forma automática, garantindo segurança, agilidade e eficiência;

- o Sistema de Escrituração Fiscal da Secretaria da Fazenda do Estado de Pernambuco, que obriga que os lançamentos de registro de operações e prestações relativas ao ICMS sejam feitos através de arquivo eletrônico assinado de forma digital, que incorpora uma série de benefícios, tais como: entrega de vários documentos em uma única remessa, redução drástica no volume de

erros de cálculo involuntário, eliminação de múltiplas escriturações, redução de custos de escrituração e armazenamento de livros fiscais, etc.;

- sistema de encaminhamento de Petições Eletrônicas no TRT-4 do Rio Grande do Sul, agilizando o tempo de cada processo de forma segura e econômica;

- o sistema PUBNet da Imprensa Oficial de São Paulo, que automatiza por completo todo o ciclo de publicações na internet de forma segura e rápida, evitando-se congestionamentos telefônicos anteriormente registrados com constância. Também foi possível, através do uso da certificação digital, a criação do e-diário oficial, que é o Diário Oficial em formato eletrônico.

#### Certificação Digital no Estado de Minas Gerais

Recentemente, a administração pública estadual identificou a necessidade de automatizar determinados processos de tramitação de documentos em sua esfera, necessitando, portanto, de ferramentas capazes de, eletronicamente, controlar o fluxo dos documentos com segurança, garantia de autenticidade e autoria, bem como com garantia de sigilo em determinados processos protegidos pela legislação em vigor.

Com base em tais requisitos, optou-se, como não poderia deixar de ser, por tecnologias envolvendo certificados digitais para pessoas físicas e jurídicas, em suas interações com o poder público estadual.

Foram consideradas as possibilidades existentes no mercado

como a criação de uma infra-estrutura de chaves públicas (ICP) estadual, baseada em certificados digitais próprios do Estado, bem como a sua adesão à ICP-Brasil.

Essa adesão foi decidida em função da garantia de validade jurídica nos relacionamentos eletrônicos conforme disposto no texto da Medida Provisória 2.200-2, bem como pelos fatores técnicos de segurança, já que a ICP-Brasil possui regras rígidas para credenciamento, com auditorias regulares, aumentando, dessa forma, a credibilidade dos certificados emitidos.

Avaliando-se as várias alternativas técnico-econômicas apresentadas, optou-se pela adesão do Estado à ICP-Brasil, por intermédio da contratação de uma autoridade certificadora de primeiro nível, ou seja, diretamente subordinada à raiz da ICP-Brasil, que terceirizaria as atividades relacionadas à infra-estrutura de segurança necessária ao desempenho das funções relacionadas à emissão dos certificados, bem como pela guarda da chave primária da AC estadual.

Através da instauração de um grupo de trabalho específico para deliberar sobre o assunto, ficou determinado que seria a Prodemge a Autoridade Certificadora do Estado.

Através de um processo licitatório, a Prodemge contratou a empresa Certisign como a provedora da infra-estrutura necessária. Cumpridas as determinações do ITI, foi publicado o Despacho da entidade, reconhecendo formalmente a Prodemge como Autoridade Certificadora e Autoridade de Registro, dentro dos padrões

da ICP-Brasil.

Várias iniciativas estão em curso no Estado para a utilização de certificados digitais em aplicações do Governo de Minas Gerais, principalmente aquelas que possibilitem a desburocratização dos procedimentos usuais das empresas e cidadãos nos seus relacionamentos com o Estado.

Podemos destacar, entre essas iniciativas, as seguintes:

- tramitação segura de documentos (Workflow) entre os diversos segmentos governamentais, garantindo maior agilidade, segurança e redução de custos pela diminuição da burocracia;

- digitalização / Gestão Eletrônica de Documentos da Junta Comercial do Estado de Minas Gerais, propiciando uma redução expressiva de documentos, aumentando a segurança e reduzindo o tempo de acesso às informações armazenadas;

- registro eletrônico de alterações contratuais via Web na Junta Comercial do Estado de Minas Gerais, aumentando a segurança, reduzindo o tempo de atendimento e a necessidade de deslocamentos ao local;

- relacionamento seguro, através de certificados, da Secretaria da Fazenda do Estado de Minas Gerais com contribuintes de ICMS, possibilitando o envio e consultas de informações de forma segura e identificada;

- relacionamento seguro de fornecedores do Estado, agilizando os processos de compras e aquisições, em especial com a Secretaria de Planejamento e Gestão, responsável por um volume sig-

nificativo de licitações;

- relacionamento seguro dos servidores estaduais com as diversas instituições, em especial com a Secretaria de Estado de Planejamento e Gestão e o Instituto de Previdência Estadual, possibilitando maior agilidade no atendimento, com redução de custos devido a um maior controle;

- identificação segura dos usuários de sistemas corporativos computadorizados, garantindo segurança e transparência nas atividades do Estado;

- comercialização segura de documentos sob responsabilidade da Imprensa Oficial do Estado de Minas Gerais;

- utilização de correio eletrônico com assinatura por todos os servidores estaduais.

As melhorias incorporadas, com a utilização da certificação digital, nos diversos aplicativos existentes ou em desenvolvimento no Estado de Minas Gerais adicionarão celeridade aos diversos processos, bem como trarão ainda maior transparência às ações da administração pública estadual.

Necessária. Cumpridas as determinações do ITI, foi publicado o Despacho da entidade, reconhecendo formalmente a Prodemge como Autoridade Certificadora e Autoridade de Registro, dentro dos padrões da ICP-Brasil.

**Caro Leitor,**

Há alguns meses, quando decidimos lançar uma revista técnica, com a chancela da Prodemge, estabelecemos de imediato um compromisso: criar uma publicação relevante, que tivesse um destino outro que enfeitar mesinhas de ante-salas de repartições. O maior temor num projeto como esse era de que, depois de pronto, soasse como uma mera reverência às vaidades de uma estatal que atua no ramo da tecnologia.

Definimos então, como premissa editorial, a concentração exclusiva em temas que estivessem na ordem do dia dos usuários, atuais ou potenciais, da tecnologia da informação. Além disso, a abordagem deveria buscar o tom exato entre a profundidade e a leveza. A primeira, deveria torná-la referência de pesquisa para usuários, técnicos e executivos em busca de conhecimentos para ajudá-los em suas decisões e estudantes em busca da última palavra sobre os temas em pauta. A segunda, cuidaria de que fosse uma publicação agradável, rica e informativa, capaz de despertar também a atenção do público interessado, mas não especializado, importante já que numeroso e formador de opinião.

Este primeiro número de Fonte reflete bem essas diretrizes.

O tema não poderia ser mais atual: Certificação Digital.

É assunto novo, com vastas áreas ainda em discussão, e que certamente provocará, em futuro próximo, profunda revolução nos costumes da sociedade em geral e, principalmente, na administração pública, com reflexos simplificadores sobre a vida dos cidadãos. Abordamos todos os seus aspectos: os legais, os técnicos, os administrativos e os culturais. Buscamos como colaboradores as maiores autoridades em cada setor, que contribuíram com entrevistas exclusivas ou textos inéditos. Procuramos, sem a pretensão de esgotar o assunto, refletir o panorama mais atual do estágio em que se encontram as discussões sobre o tema no País.

Temos a consciência de que o que apresentamos agora não é um produto acabado. Por isso, abrimos uma seção para interação com os leitores. Dela, tiraremos sugestões, ouviremos críticas e, eventualmente, buscaremos inspiração para possíveis e oportunas correções de rumo.

Finalmente, analisando este primeiro número de Fonte, que agora publicamos, temos a esperança de termos escapado da irrelevância.

No entanto, submetemos esta avaliação ao julgamento soberano - na realidade o que realmente importa - dos nossos leitores.

Um abraço,

**Maurício Azeredo Dias Costa**

Uma Publicação da:



Ano 1 - nº 1 - Dezembro de 2004

**Governador do Estado de Minas Gerais**  
Aécio Neves da Cunha  
**Secretário de Estado de Planejamento e Gestão**  
Antonio Augusto Junho Anastasia  
**Diretor-Presidente**  
Maurício Azeredo Dias Costa  
**Diretora de Projetos e Negócios**  
Glória Maria Menezes Mendes Ferreira  
**Diretor de Tecnologia e Produção**  
Raul Monteiro de Barros Fulgêncio  
**Diretor Administrativo e Financeiro**  
José Ronaldo Fidelis  
**Diretor de Desenvolvimento Empresarial**  
Nathan Lerman

## Fonte

### CONSELHO EDITORIAL

Antonio Augusto Junho Anastasia  
Maurício Azeredo Dias Costa  
Márcio Luiz Bunte de Carvalho  
Amílcar Vianna Martins Filho  
Gustavo da Gama Torres  
Paulo Kléber Duarte Pereira  
Marcos Brafman

### EDIÇÃO EXECUTIVA

Assessoria de Comunicação  
Pedro Marcos Fonte Boa Bueno  
Edição, reportagem e redação  
Isabela Moreira de Abreu - MG 02378 JP  
Coordenação do projeto editorial, gráfico e publicitário  
Gustavo Grossi de Lacerda  
Universidade Corporativa Prodemge  
Enilton Rocha Ferreira  
Marta Beatriz Brandão P. e Albuquerque  
Luiz Cláudio Silva Caldas  
Projeto gráfico, capa, ilustrações, diagramação  
e editoração gráfica  
Guydo José Rossi Cardoso de Menezes  
Estágio programação visual  
Camila Maciel Leite Seabra  
Revisão  
Fátima Campos  
Fotolito e impressão  
Policron / Gráfica Formato  
Tiragem  
Três mil exemplares  
Periodicidade  
Semestral

### PATROCÍNIO

Esta edição da revista contou com o apoio:



**Prodemge - Rua da Bahia, 2277 - Bairro Lourdes  
CEP 30160-012 - Belo Horizonte, MG, Brasil**  
[www.prodemge.mg.gov.br/](http://www.prodemge.mg.gov.br/) / [prodemge@prodemge.gov.br](mailto:prodemge@prodemge.gov.br)



**Fonte**



---

# Sumário

---

**Fonte**

Número 01 - Dezembro de 2004

**prodemge**

Tecnologia de Minas Gerais

---

- 03** **Interação:** comentários e sugestões de leitores
- 04** **Diálogo:** entrevista com o advogado-geral do Estado de Minas Gerais, José Bonifácio Borges de Andrada, que fala dos aspectos histórico e jurídico da certificação digital no País
- 11** **ICP-Brasil: Evolução com Equilíbrio e Correção** - o diretor do ITI, Evandro Oliveira, aborda o comportamento do mercado frente à consolidação da certificação digital
- 13** **Governo Eletrônico: Projeto de Segurança da Informação do Governo Mineiro** - a secretária-adjunta de Planejamento e Gestão do Governo do Estado de Minas Gerais, Renata Vilhena, comenta o desafio da segurança da informação com o uso crescente da tecnologia
- 14** **A Criptografia na Ficção** - técnicas antigas e fantasias modernas no artigo do analista de sistemas da Prodemge, Luís Carlos Silva Eiras
- 16** **Dossiê:** panorama da certificação digital - aplicações, benefícios, perspectivas e a opinião de autoridades no assunto
- 32** **Benchmarking:** duas experiências de sucesso - a Receita Federal e o Tribunal Regional do Trabalho 4ª Região (RS)
- 35** **Fórum:** a certificação digital e os cartórios - o professor de Ciência Política, José Eisenberg, comenta o desafio que a certificação digital representa para o futuro da burocracia
- 37** **Universidade Corporativa Prodemge:** seleção de artigos acadêmicos inéditos sobre os temas certificação digital e segurança da informação
- Considerações sobre a interoperabilidade aplicada à infra-estrutura de chaves públicas - Fabiano Menke
- A privacidade na ICP-Brasil - Alexandre Rodrigues Atheniense
- Tudo que você deve saber sobre certificação digital - Jeroen van de Graaf
- Certificação digital: uma realidade em Minas - Raymundo Albino e Sérgio Daher

---

# Interação

---


Este espaço é  
destinado a acolher  
as opiniões e  
sugestões de  
nossos leitores.

Participe, contribua,  
faça contato:  
seu retorno é  
fundamental para  
que a  
revista evolua a cada  
edição.

---

**e-mail:**  
**[revistafonte@prodemge.gov.br](mailto:revistafonte@prodemge.gov.br)**

---



Rua da Bahia, 2277, Lourdes -  
Belo Horizonte, MG - CEP:  
30160-012, aos cuidados da  
Assessoria de Comunicação da  
Prodemge - Companhia de  
Tecnologia da Informação do  
Estado de Minas Gerais.

### Segurança e armazenamento de documentos: da inscrição na pedra à Certificação Digital



**José Bonifácio Borges de Andrada, advogado-geral do Estado/MG. Dentre os vários cargos públicos que exerceu, foi advogado-geral da União, subsecretário-geral da Presidência da República, secretário-executivo do Ministério da Justiça, subchefe para assuntos jurídicos da Casa Civil da Presidência da República e consultor jurídico do Ministério da Previdência e Assistência Social. Tem o cargo efetivo de procurador regional da república.**

Na primeira edição da Revista Fonte, o entrevistado é o advogado-geral do Estado, José Bonifácio Borges de Andrada. Com larga experiência no setor público, no qual ocupou importantes cargos nos governos Federal e Estadual, e também com grandes conhecimentos na área de tecnologia da informação, o advogado-geral do Estado teve participação decisiva na criação da Infra-Estrutura de Chaves Públicas do Brasil – ICP-Brasil, atuando primeiramente como consultor jurídico do Ministério da Previdência e Assistência Social, onde surgiram as primeiras evidências da necessidade de mecanismos de proteção às informações eletrônicas; e, posteriormente, como subsecretário-geral da Presidência da República e advogado-geral da União, quando foi finalmente estabelecida a Medida Provisória 2200, que regulamenta a certificação digital no Brasil.

Nesta entrevista, José Bonifácio traça, de forma didática, um panorama histórico da certificação digital no País e fala, com propriedade e bom humor, das perspectivas dessa tecnologia no Brasil. Ele refuta o mito de seu uso explosivo no comércio eletrônico e pontua os benefícios de sua utilização para o setor público, enfatizando a experiência em Minas, onde a tecnologia tornou-se realidade em 2004 .

**Fonte: Como surgiram as primeiras iniciativas para estabelecer o serviço no Brasil?**

“Eu fui despertado para essas questões de informática, do ponto de vista legal, quando trabalhava no Ministério da Previdência. Algumas fraudes vinham sendo feitas no sistema ou através do sistema. Algumas, muito primárias, muito simples; outras, devido à falta de cuidado de pessoas que deixavam seu cartão magnético com a senha pregada com durex na tela do computador, para facilitar o serviço. Havia no entanto outras mais complexas, mais elaboradas, que exigiam um pouco mais de conhecimentos. Houve um dia em que um hacker conseguiu fazer clone da página da Previdência e colocou informações para confundir as pessoas. A nossa sorte é que ele colocou um Fale Conosco. Mandamos então um e-mail para ele, dizendo que a Polícia estava chegando. Conseguimos resolver o problema e tirar a falsa página do ar.

Com esses episódios, chegamos à conclusão de que era necessária uma legislação criminal específica para a área previdenciária. Elaboramos então algumas alterações no Código Penal, que estão em vigor hoje, para a proteção da base de dados da Previdência. Esse projeto foi encaminhado ao Congresso. Nesse meio tempo, eu fui convidado para trabalhar na Casa Civil e o projeto tramitava no Congresso.

Na Casa Civil, nós temos um contato maior com a estrutura de Governo e começamos a perceber que a demanda era comum a todos os outros órgãos.”

**Fonte: Naturalmente, houve necessidade de adequações na Lei. Como foi conduzido o processo?**

“Percebemos que todos os órgãos tinham dados e informações que precisavam ser preservados e que o projeto da Previdência, que estava mais avançado, na verdade servia para todo mundo. Fizemos então algumas alterações no Projeto de Lei que estava na Câmara e o adequamos para a administração pública. Foram então criados, pela primeira vez, alguns crimes específicos, que estão no Código Penal. Isso é importante também: não fizemos uma lei específica, fizemos alterações no Código Penal, que é a lei penal comum, que todo mundo usa, a lei básica criminal do País, protegendo documentos e informações constantes em bases de dados e também criando algumas hipóteses criminais de invasão de bases de dados.

Por exemplo, ceder senha de acesso a um banco de dados protegido a um terceiro, em certos casos, é crime. Uma pessoa não pode passar informalmente a senha a uma pessoa não autorizada. Só passar a senha já é crime. Se isso significa uma invasão a uma base de dados, é um outro crime com pena mais grave. Se, da invasão, resulta um dano à base de dados, aí é outro crime, com pena mais alta ainda. Não estávamos ainda na fase da certificação digital. Mas chegou-se a um ponto em que houve demanda pela certificação digital.”

**Fonte: Nessa época, como outros países conduziam a questão da segurança de seus documentos eletrônicos?**

“Nessa época, ou um pouquinho antes, a Europa já tinha feito uma diretriz para a União Européia. Uma diretriz básica que orientava todos os países sobre como regulamentar a certificação digital na Europa.

Outros países também estavam fazendo uma legislação própria. Nos Estados Unidos, bem no seu estilo – devido à liberdade de cada Estado –, cada um definia

**“Foram estudados os modelos do mundo e o governo optou por adotar o modelo vigente na Comunidade Européia...”**

sua forma de atuação mais conveniente. Mas o assunto estava em fase de organização, por volta de 1999/2000.

E nós sentimos a necessidade de que houvesse aqui no País também alguma forma de regulamentação. Nós, da área jurídica, conhecíamos pouco sobre o assunto; tivemos que estudar, porque não conhecíamos, naturalmente, a legislação, a prática e os mecanismos de funcionamento da certificação digital. Tivemos que nos informar, estudar muito, contando com a ajuda de especialistas. O professor Miguel

Teixeira Carvalho, do Ministério da Ciência e Tecnologia na época, e o pessoal do Serpro nos ajudaram muito no entendimento da certificação digital e os conceitos de chave pública, chave privada, algoritmo de hash e outros. E, ao entender a certificação digital, tivemos também que entrar no conceito de Autoridade Certificadora e Autoridade Raiz, o que foi muito importante para depois estabelecer o modelo.”

**Fonte: O senhor participou ativamente da concepção da ICP-Brasil, ajudando a definir o modelo de certificação que foi adotado no País. Como foi feita essa escolha?**

“O modelo de certificação digital que o Brasil adotou está na Medida Provisória 2200. Foram estudados os modelos do mundo e o Governo optou por adotar o modelo vigente na Comunidade Européia, previsto na Diretiva 93/1999, por dois motivos: primeiro, devido à similitude da legislação – a nossa legislação é uma herança do sistema romano-germânico, nossas leis são baseadas nas leis portuguesas, espanholas, italianas, e sofrem muita influência do direito alemão. A maneira de legislar brasileira, a nossa maneira de agir no processo judicial, é muito mais próxima do sistema europeu. Chegamos à conclusão de que seria, portanto, mais fácil para o mundo jurídico brasileiro assimilar, com mais rapidez, um conjunto de normas que tivesse uma sistemática européia do que uma sistemática americana.

O segundo motivo é que a sistemática européia é compatível com a sistemática americana, mas o contrário não ocorre. Se

adotássemos o modelo europeu, o sistema brasileiro conversaria com os americanos; mas se adotássemos o modelo americano, teríamos dificuldades para conversar com os europeus. É que a Diretiva Européia 93/1999 dá padrões mínimos básicos de organização do sistema, mas, ao mesmo tempo, ela tem que ser flexível o suficiente para respeitar as diversidades culturais de cada país. A Diretiva, portanto, não poderia ser muito rígida.

Resumindo, as coisas funcionam mais ou menos assim: na medida em que nós respeitamos a Diretiva Européia, passamos a ser como “um membro da comunidade européia”. Se os sistemas dos vários países falam entre si, falam também com o nosso. Isso, para negociações futuras, facilita nosso ingresso na Europa; e o sistema americano é absolutamente aberto, na realidade, aceita qualquer um.”

### **Fonte: O que exatamente determina a Medida Provisória 2200?**

“A opção do Governo está sintetizada na MP-2200, que prevê dois sistemas paralelos, que operam simultânea e livremente: um sistema de certificação livre e um sistema de certificação governamental.

Para este, foi criada a Autoridade Raiz única – que é o ITI –, uma autarquia federal, a Infra-Estrutura de Chaves Públicas hierarquizada, dentro da estrutura da ICP. A MP estabeleceu ainda que a Autoridade Raiz não tem contato com o usuário, quer dizer, ela não é a fornecedora do certificado no nível do usuário; ela certifica as autoridades certificadoras de segundo nível, que

podem ser órgãos públicos ou privados. Ou seja: a MP criou o modelo da infra-estrutura e fixou as atribuições legais do sistema público e privado, copiando rigorosamente a Diretiva Européia.”

### **Fonte: Faça, por favor, um paralelo entre uma operação apoiada pela ICP-Brasil e uma feita fora dessas regras.**

“Em pouquíssimos casos, há a obrigatoriedade de se trabalhar com a autoridade pública. Na prática, é o seguinte: se você trabalha com a ICP-Brasil e assina um documento eletrônico, você não pode negar que assinou o documento. E a parte do outro lado tem o direito de presumir que você o assinou. Se você quiser dizer que aquele documento não foi assinado por você, você tem que fazer a prova. É a presunção de autoria. É uma operação mais segura, porque equivale a uma operação com testemunhas. A Autoridade Raiz e a Autoridade Certificadora são testemunhas de que você é você – o Governo certifica que você é você e a Lei presume que você é o autor do documento.

Fora da ICP, acontece o contrário: se a outra parte duvidar da autoria, cabe ao emitente provar a autenticidade de sua assinatura. As operações são mais tranquilas e mais rápidas porque a outra parte aceitará a sua assinatura se quiser; se não quiser, ela não concorda que você assinou e não faz a operação. E se ela questionar a sua assinatura, você é que tem que provar que ela é autêntica.

Fora da ICP, você não terá uma autoridade: você terá uma

testemunha privada que as partes aceitarão se e na medida em que quiserem. Por exemplo, duas empresas podem contratar uma certificadora privada e fazer negócios, sem problema nenhum, fora da PKI ou ICP oficial.”

### **Fonte: Na prática, como o mercado assimilará esses dois sistemas paralelos?**

“Eu acredito que será o seguinte: na maioria das operações comerciais de baixo valor, você não usará certificação nenhuma, permanecerá como está funcionando atualmente, com cartões de crédito, por e-mail por exemplo. Eu não vou querer comprar um cartão de certificação para isso. E o entregador de gás ou pizza também vai continuar da mesma forma. A certificação seria um custo a mais.

Para as operações de porte médio, eventualmente as empresas vão contratar infraestrutura particular. Não será necessário entrar na esfera governamental, que é mais cara porque a segurança é maior. Se você não precisa de muita segurança, não há motivo para aumentar o custo.

Agora, para documentos oficiais, para os quais a Lei exige autenticidade, aí, nesses poucos casos, você será obrigado a entrar no sistema da ICP-Brasil; ou ainda se o valor das operações for muito alto ou se, por segurança, as partes optarem também pela ICP-Brasil. E as empresas certificadoras também têm inteira liberdade. A mesma empresa pode oferecer serviços dentro da ICP e fora da ICP.

O que vai acontecer é que a certificação emitida pela ICP-



Brasil vai custar mais caro; fora do sistema, a empresa não vai precisar pagar taxas por esse documento, não é submetida à fiscalização e não é exigido dela um certo padrão de qualidade, como a ICP-Brasil, que tem padrão internacional. A nossa Autoridade Raiz – que é o ITI – tem que estar e está no mesmo padrão de qualidade da Europa.”

**Fonte: Comente a certificação digital como solução para a questão da segurança. Como esse expediente se contrapõe ao uso do documento em papel?**

“No fundo, nós convivemos com o uso da correspondência eletrônica em grande escala: hoje, você troca muito e-mail, muita correspondência por computador. Além do e-mail, há também o sistema de mensagem direta, que são os messengers, e o sistema de imagem também – brevemente a certificação vai ter que contemplar a imagem. Daqui a pouco, você vai ter a conversa na internet com som e imagem, gravá-los em CD e com possibilidade de certificação do CD.

A partir de um determinado momento, a comunicação pela internet perde a confiabilidade. Isso acontece mais ou menos como com o telefone e com o fax. Ninguém compra, por exemplo, uma casa por telefone. Tanto vendedor quanto comprador vão querer tudo bem escrito, documentado, com testemunhas, em cartório. Há o serviço de telepizza – por telefone –, mas não há o telecasa. Há vários serviços de comércio por telefone. Mas algumas operações, a partir de um certo valor, você não vai fazer por telefone. Você vai querer se certificar da operação.

Em geral, a certificação se faz em papel: você faz um contrato, busca testemunhas, registra em cartório. Na verdade, a certificação digital não se dirige para a grande massa de operações comerciais. É um engano achar isso. Funciona da mesma forma que a certificação em papel, que você faz para operações de grandes valores, duradouras. Assim como você não faz a compra de uma casa ou apartamento, por telefone, você também não faz uma escritura pública para comprar um sanduíche. Ali é importante justamente que não tenha a certificação. Porque ela torna o

**“Na verdade, a certificação digital não se dirige para a grande massa de operações comerciais. É um engano achar isso.”**

processo mais lento e, nos negócios de grande escala, de pequeno valor unitário, você quer velocidade, e a certificação vai atrapalhar isso. A relação custo-benefício faz valer a pena o risco.

Para ilustrar: quando você pede uma entrega de gás, por telefone, você pode estar falando com o Jack, o Estripador. Há uma possibilidade mínima de não ser o entregador de gás. Da mesma forma que o rapaz do gás pode estar recebendo o telefonema do Jack, o Estripador. Se, toda vez que se fizer uma operação dessa natureza, for exigido documento de identidade, ou outros, ele não vai vender nenhum botijão de gás.

Ele, portanto, tem que correr algum risco.

Isso vale, da mesma forma, para a compra de uma passagem aérea pela internet: você quer facilidade, velocidade, portanto, não se usa a certificação. E tem funcionado. A empresa aérea que exigir que o cliente tenha um cartão, um token ou um outro elemento de certificação está criando um complicador para o cliente. E o que ela quer é facilitar. Isso já vale até para os cartões de crédito. Já se dispensa, em muitos casos, a assinatura do titular, bastando informar o número do cartão. O cartão já dispensou a certificação – que é a nossa assinatura – para ganhar tempo.”

**Fonte: Em que casos, então, a certificação é a solução mais indicada?**

“Ela entra quando você quer ter perenidade e durabilidade na informação, para que outros possam saber que a operação foi feita. A operação ou o documento será armazenado por longo tempo, como alguns documentos públicos ou por exigência legal. Ou quando o valor da operação é tão grande que você deseja uma segurança a mais.

Enfim, a certificação não é nada mais nada menos que um processo de autenticação, não do documento, mas da autoria do documento. Em algumas operações, você tem que saber com certeza com quem está falando, quem está enviando a mensagem. Em outras, você não precisa ter certeza; você presume a certeza. A quantidade de ligações telefônicas que fazemos, e-mails e fax que transmitimos mostra que a maioria das mensagens que

trocamos dispensa um tipo de certificação mais séria. Em geral, você se contenta com o nome da pessoa no cabeçalho do e-mail, o que é facilmente falsificável.

A estrutura da ICP-Brasil funciona para uns poucos casos em que é obrigatória. Fazendo um paralelo: quando é que nós somos obrigados a ir a um cartório passar uma escritura? Em pouquíssimos casos.

Na maioria das vezes, nós fazemos os nossos negócios por documentos particulares. A ICP, da mesma forma, é obrigatória em um número limitadíssimo de casos e ela faz uma remissão para o Código Civil Brasileiro. Na maioria dos casos, a ICP não é obrigatória: você pode trabalhar com ICPs particulares, privadas e fora do sistema governamental.”

**Fonte: Com relação ao comércio eletrônico, há uma grande expectativa de aquecimento nesse tipo de transação. Essa expectativa é procedente?**

“Fala-se muito em comércio eletrônico. É um engano pensar que a certificação digital é importante para o comércio eletrônico. Na verdade, o comércio eletrônico em geral não vai usar a certificação, ou vai usar muito pouco. Na minha opinião, é muito importante para a maioria das transações comerciais justamente que não haja o processo de certificação, a fim de agilizar esse tipo de operação.”

**Fonte: Na prática, como funciona no setor público o uso da certificação digital?**

“No Governo Federal, desde 2000, as correspondências

oficiais dos ministros ao Presidente da República – propondo projetos de lei, projetos de decretos, minutas de medidas provisórias – são feitas, transmitidas e assinadas eletronicamente. Cada ministro de Estado tem seu cartão, sua senha, e os documentos são transmitidos para a Casa Civil com a garantia de autenticidade não do transmissor da mensagem, mas do autor do documento.

A certificação digital substitui a assinatura em papel. E quem recebe o documento tem a mais absoluta certeza de que foi produzido por determinado ministro, por determinada autoridade. Não se faz mais esses documentos em papel.

A Casa Civil, inclusive, recusa quando feitos em papel. Era assim nos dois últimos anos do governo Fernando Henrique, mas acho que não mudou a sistemática. Cada ministro de Estado, cada secretário de Ministério tem a sua senha, que é o seu cartão magnético, é um cartão com um chip contendo exatamente a chave privada com um algoritmo.”

**Fonte: Como será a aplicação da certificação digital em Minas?**

Será a mesma coisa: temos aqui a Advocacia Geral, a transmissão de documentos oficiais para o Palácio, a transmissão de documentos do Palácio para a Imprensa Oficial. Hoje é necessário adotar as duas formas: envia-se o documento por meio eletrônico, mas, por segurança, o papel vai atrás. Quando tivermos a certificação digital, vamos acabar com o papel. Vamos ganhar tempo.”

**Fonte: Sintetize, por favor, os benefícios da certificação digital para a administração pública.**

“Você ganha velocidade na transmissão da informação eletrônica; já tem isso, mas você passa a transmitir dados e documentos por meio eletrônico que você não poderia fazer se não estivesse na ICP-Brasil.

Não se pode, hoje, mandar um documento oficial para o governador e não assinar; eu tenho que assinar, qualquer secretário que mandar um documento oficial tem que assinar.

Não se pode, hoje, mandar um documento oficial para o governador por e-mail, ainda que o governador se disponha a receber esse e-mail.

Primeiro, o governador tem um problema de segurança: ele não sabe se quem está passando aquele e-mail é o próprio secretário ou um auxiliar dele; segundo, ele não tem certeza quanto à autenticidade do documento: ele não sabe se o documento foi modificado no meio do caminho ou se o documento não foi modificado no seu próprio computador. Com a certificação, se ele estiver assinado e alguém fizer alguma alteração, essa assinatura cai; saberemos que esse documento sofreu uma alteração.

Ganhamos na velocidade e eliminamos o office-boy em muitas circunstâncias. Ganhamos na velocidade, no tempo, na distância.”

**Fonte: Quais são as vantagens de uma entidade pública no processo de**

## **certificação digital?**

“Com a certificadora pública, você passa a ter um pouco mais de liberdade. No caso da Prodemge, por exemplo, como uma Autoridade Certificadora dentro da ICP-Brasil, passamos a ter a liberdade de, nós mesmos, emitirmos os nossos certificados, tendo as nossas autoridades de registro. Mas, provavelmente, a Prodemge não vai entrar no mercado privado para competir com empresas privadas de certificação, mesmo porque o perfil dela é voltado para servir ao Estado.

Isso equivale mais ou menos também àquela história: o Estado pode ter ou não a sua própria companhia de energia elétrica; Minas tem a Cemig. Não sei se outros estados têm, mas nem por isso o pessoal de lá está no escuro. É claro que você, tendo o serviço próprio, passa a ter uma certa liberdade. Não é bom nem ruim, depende da conveniência.”

**Fonte: Como o senhor avalia a questão da tradição do uso do documento em papel, que é algo palpável, com a entrada do documento digital, através da certificação?**

“O papel não vai acabar. Na medida em que você certifica um documento eletrônico, você passa a poder armazená-lo com segurança. Não com segurança da duração do armazenamento, mas com segurança da autenticidade do documento. Uma coisa é você achar um papel velho; outra é você achar um papel velho com uns rabiscos e uma assinatura do Beethoven embaixo. Ah, isso aqui é o original da Quinta Sinfonia!

Na medida em que o papel passou a ser assinado, ficou importante ele ser guardado. Da mesma forma, na medida em que o documento eletrônico possa ser assinado, pode-se armazenar esse documento, ele começa a ficar importante, porque ele passa a ter o valor do papel assinado. Recentemente, entreguei ao Arquivo Público Mineiro algumas dezenas de metros de papéis que eram originais de decretos desde mais ou menos 1940 até hoje. Eram os originais, que estavam guardados aqui porque são produzidos aqui. Se, mais tarde, o governador estiver fazendo assinaturas eletrônicas de decretos, eu não vou ter decretos aqui,

**“Os documentos do Qumran duraram 2 mil; estão arquivados há 2 mil anos. Não sabemos se daqui a 500 anos alguém vai ler um disquete.”**

arquivados em papel, mas arquivados eletronicamente. Ao invés de metros de papel, eu vou ter alguns centímetros de CDs numa caixinha, que eu posso, inclusive, duplicar e enviar para o arquivo até pela internet.”

**Fonte: Com relação à mídia de armazenamento dessas informações e documentos, o senhor se preocupa com os meios de recuperação das informações. Comente esse aspecto.**

“Temos que considerar as

mesmas dificuldades de um microfilme, por exemplo. Eu tenho em minha casa algumas dezenas de LPs antigos e tenho lá um toca-discos que está sem agulha. Eu estou atrás de uma agulha para esse toca-discos. Todos já estão duplicados em CD, mas eu gosto do LP. Ou seja, a minha mídia está ficando ultrapassada. Quem guardou alguma coisa naqueles disquetes de 5 ¼ e não passou para outra mídia perdeu informação. Vai ter que ir a um museu para recuperá-los – você vai ter que trabalhar com a arqueologia eletrônica. Há essas susceptibilidades. Não vamos pensar que o meio eletrônico é a grande solução. Ele tem problemas. Obviamente, na sepultura dos nossos parentes, nos cemitérios, nós vamos continuar colocando o nome na pedra, no mármore, porque nós queremos que isso dure muito. Ninguém vai largar um chip na sepultura.

A pedra é uma das mídias mais duráveis que já se descobriu. O homem da pedra descobriu, quando começou a escrever, que tratava-se de uma mídia durável. Não era só porque não tinha o papel. Não é prático, mas tem muita escrita em pedra que recuperou a nossa história. Nós não sabemos a durabilidade de um CD. A carta de Pero Vaz de Caminha já durou 500 anos; nós não sabemos se a mídia eletrônica se conserva por 500 anos. Os documentos do Qumran duraram 2 mil; estão arquivados há 2 mil anos. Não sabemos se daqui a 500 anos alguém vai ler um disquete.

A certificação permite que você passe a ter um armazenamento importante de informações, mas, eventualmente, como não é um armazenamento físico, você tem

um problema de recuperação. É mais fácil recuperar informação de um LP do que de um DVD ou de um disquete de computador, em que o armazenamento é lógico.

A certificação digital valoriza muito o armazenamento da informação eletrônica, porque ele passa a ser um armazenamento com alto grau de confiabilidade quanto à autenticidade. Ela agrega valor ao documento. Mas a certificação não acrescenta nada com relação à durabilidade. Mesmo a certificação privada, é importante, por exemplo, para documentos históricos particulares. A carta de Pero Vaz de Caminha é um documento oficial, tratava-se de um escrivão do rei na esquadra, uma autoridade pública.

De outra forma, são documentos particulares os Lusíadas, Odisseia, a Ilíada. Mesmo a certificação privada agregará valor a documentos privados arquivados com certificação digital privada.”

**Fonte: *Sistemas da Microsoft estariam adaptados para o sistema brasileiro de certificação digital. Como funciona?***


“No caso da chave pública brasileira, foi assinado, em 2002, um convênio entre o Governo brasileiro e a Microsoft. A partir daquela data, a chave pública brasileira estaria fazendo parte do sistema da Microsoft. Nós somos um dos poucos países do mundo a fazer esse acordo com a Microsoft. Como funciona: para usar o sistema de certificação, no seu computador, há o sistema de senha e contrasenha e o seu computador tem que conhecer a contrasenha da autoridade

certificadora da autoridade raiz, ou seja, essa contrasenha tem que estar nos sistemas, é a chave pública.

Se ela não estiver nos sistemas, você vai ter que baixá-la no computador. Se você vai trabalhar com a ICP, vai ter que entrar no site da autoridade raiz, baixar a chave pública no seu computador, armazenado-a na memória. Na hora em que você fizer comunicações usando assinaturas eletrônicas, o computador da outra parte, ao receber a sua mensagem, vai ter condições de lhe dizer que a autoridade raiz está garantindo a operação. Se isso não está no computador, você tem que fazer algumas operações manuais para consultar a raiz ou consultar a certificadora.

É mais ou menos isso: alguém me telefona e diz uma senha; você tem que dar a contrasenha. Aí você teria que ligar para uma terceira pessoa e confirmar se senha e contrasenha estão compatíveis, porque você não confia na ligação, mas você confia em quem vai lhe dar informações sobre a senha, que é a autoridade certificadora. Esse sistema pode ser on-line ou através de vários passos. Uma vez dentro do sistema da Microsoft, é como se houvesse uma linha com a raiz.

A Microsoft permite que, na hora que você colocar o sistema de senha e contrasenha ou de chave pública e chave privada no computador, a consulta seja feita automaticamente. E, no computador, você já pode saber se o documento é válido. Com esse acordo, isso já vem no sistema. A Microsoft só fez isso depois de ter uma declaração formal do Brasil de que a nossa Autoridade Raiz atende a uma série de requisitos

que ela solicitou. Eles quiseram auditar o sistema, mas isso nós não permitimos.” 



# ICP-Brasil

## Evolução com Equilíbrio e Correção

Evandro Oliveira

Após um tempo considerável, desde que a certificação digital no Brasil tomou rumos mais claros e específicos (a Medida Provisória 2.200-2 sobre o tema foi publicada em agosto de 2002), ainda encontramos pessoas que, mesmo atuando na área de informática, mesmo sendo profissionais qualificados, ainda não conhecem o funcionamento, aplicabilidade e exemplos práticos das vantagens de se ter a adoção de uma Infra-estrutura de Chaves Públicas (de PKI - Public Key Infrastructure).

Alguns casos de não reconhecimento chegam a repetir certa técnica muito utilizada noutro tema muito polemizado ultimamente, o software livre. Os desconhecidos utilizam da aplicação do medo, da incerteza e da dúvida (FUD, da expressão em inglês) quanto à eficácia e correção do processo de Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), com argumentos que são do domínio de parcela que nem mesmo discute o tema com qualidade.

Embora a ICP-Brasil preveja que particulares possam utilizar qualquer tipo de certificação, ainda são muitos os profissionais de informática que não entenderam em quais condições devem usar processos diferenciados de certificação digital. Entendemos que se os profissionais de TI passarem a usar certificados digitais, assinaturas eletrônicas, criptografia assimétrica e até mesmo criptografia

simétrica, com a preocupação de interoperabilidade entre estes mecanismos, constatarão que a estrutura adotada no Brasil é a mais apropriada aos propósitos de Governo e Setor Privado.

Mas como é natural que mais pessoas passem a questionar os processos existentes e vejam as vantagens do uso de certificação digital como um grande passo na melhoria e segurança dos

procedimentos e transações feitas por particulares e por estes e o poder público, o que estamos presenciando é uma crescente adoção e aceitação dos regulamentos previstos na MP 2.200-2 e nas resoluções publicadas pelo Comitê Gestor da ICP-Brasil.

Para começar a entender o funcionamento dessa estrutura, é necessário saber a diferença entre as formas e processos de certificação digital e a hierarquia adotada no País ([www.iti.gov.br](http://www.iti.gov.br)). O regulamento implantado determina que as regras devem

ser aprovadas pelo Comitê Gestor que tem representação do Poder Executivo Federal e da Sociedade Civil (com previsão de que os Poderes Legislativo e Judiciário passem a ter representação no referido Comitê). Este Comitê é assessorado por um Conselho Técnico que estuda e debate as questões técnicas, questões jurídicas e administrativas e adoção de tecnologias para promover a interoperabilidade entre certificados de autoridades certificadoras diferentes da estrutura.

**“Os desconhecidos utilizam da aplicação do medo, da incerteza e da dúvida quanto à eficácia e correção do processo de Infra-estrutura de Chaves Públicas Brasileira...”**



A Autoridade Certificadora Raiz, representada pelo Instituto Nacional de Tecnologia da Informação – ITI ([www.iti.br](http://www.iti.br)) –, autarquia vinculada à Casa Civil da Presidência da República, cuida para que a operação das autoridades certificadoras, autoridades de registro, prestadores de serviço, auditorias independentes e demais intervenientes possam atuar na estrutura com as melhores condições e funcionalidades.

As empresas da iniciativa privada e órgãos públicos já estão se posicionando de forma a escolher onde estão mais aptos e adequados a atuar com certificação digital na estrutura da ICP-Brasil e, após serem auditados para mostrar conformidade com as regras estabelecidas, recebem o credenciamento e podem atuar com os demais e servindo ao cidadão com garantias que não presenciemos em métodos de certificação não auditáveis. Cabe então a cada um desses intervenientes estudar o tema, se apresentar como capaz para desempenhar o papel que deseja e, após credenciado, se qualificar como debatedor e participe da evolução do processo.

Confiar que a estrutura estabelecida pode determinar as técnicas e tecnologias a serem adotadas e que as auditorias são realizadas com intuito de verificar o proposto e realizado pelas entidades credenciadas é mais importante do que não participar e querer que um ponto aqui e outro acolá seja modificado para atender interesses corporativos e particulares.

As regras de ICP-Brasil têm evoluído a partir da primeira estrutura montada, e devemos ressaltar

que é importantíssimo não “jogar fora” o investimento valioso já implementado e em uso no País. Não se deve nem imaginar o estrago que poderia ser feito se o Sistema de Pagamentos Brasileiro, o maior exemplo do uso prático da certificação digital no País, tivesse que ser refeito. Outro exemplo a ser referenciado daqui a alguns dias é o uso integral, por parte dos servidores da Receita Federal, de certificados digitais da ICP-Brasil.

Trabalhamos para, a cada reunião do Comitê Gestor, propor revisões que consolidem, cada vez mais, a inserção de instituições do setor público que não sejam da esfera federal, não pelo método do medo, incerteza e dúvida, mas por contribuirmos para que todos acreditem que estão fazendo a escolha por sistemas criptográficos apropriados e, a partir daí, passem a contribuir com o País na adoção e aplicação das estruturas e regras da ICP-Brasil, elevando consideravelmente os níveis de segurança nas transações que utilizem as mais variadas tecnologias da informação.

**“As empresas privadas e órgãos públicos já estão se posicionando de forma a escolher onde estão mais aptos e adequados a atuar com certificação digital...”**

**Evandro Oliveira**

**Diretor de Auditoria, Fiscalização e Normalização  
Instituto Nacional de Tecnologia da Informação –  
ITI – Casa Civil – Presidência da República**



# Governo Eletrônico Seguro

## O projeto de segurança da informação do governo mineiro

Renata Vilhena

Com o crescente uso das novas tecnologias da informação e comunicação, principalmente com o advento da internet, e com a importância da informação enquanto recurso estratégico, a segurança da informação passou a ser uma das principais preocupações das organizações, sejam elas públicas ou privadas.

No que tange às organizações públicas, inserem-se, num contexto de modernização do Estado, propostas que envolvem novas tecnologias da informação e comunicação nas relações entre Governo e Cidadão (G2C), Governo e Empresas (G2B), Governo e Servidores (G2E) e Governo e Governo (G2G). Entretanto, nessas relações, é necessário um aparato que dê garantias e confiabilidade nas transações eletrônicas entre o Governo e a Sociedade.

Nesse sentido, o Governo do Estado de Minas Gerais, em consonância com o Programa de Governança Eletrônica, está promovendo ações com o intuito de desenvolver um projeto de implantação de Modelo de Gestão de Segurança da Informação na Administração Pública do Poder Executivo Estadual.

Sob coordenação da Secretaria de Estado de Planejamento e Gestão (Seplag) e em parceria com a Secretaria de Estado de Fazenda (SEF) e da Companhia de Tecnologia da Informação de Minas Gerais (Prodemge), o Projeto de Segurança da Informação tem como objetivo preparar as referidas instituições para alcançar um nível de segurança desejada.

Para tanto, serão realizadas atividades que vão desde uma ampla análise de riscos em seus ativos tecnológicos e seus principais processos de negócio

até a elaboração e divulgação de política de segurança da informação, capacitação de técnicos e campanhas de sensibilização de usuários, desenvolvimento de um Plano Diretor de Segurança da Informação e de um Plano de Continuidade de Negócios.

Outra ação de destaque diz respeito à capacitação tecnológica da Prodemge, que se tornará um Security Provider, contando com a parceria da Módulo, empresa brasileira com maior renome em segurança

da informação no País, com mais de 19 anos de existência e considerada uma das maiores empresas de segurança da informação do mundo. Pretende-se também obter a Certificação Internacional da Prodemge junto à BS 7799, norma de referência internacional em segurança da informação.

Enfim, esse projeto, em consonância com a Certificação Digital - projeto em andamento e coordenado pela Prodemge - proporcionará ao Governo do Estado infra-estrutura de tecnologia da informação e comunicação e processos de negócios seguros. Dessa forma, a Administração Pública do Poder

Executivo Estadual estará apta para a prestação de informações e serviços eletrônicos de forma segura, fortalecendo os mecanismos de participação dos cidadãos e transformando as relações entre Estado e Sociedade, condição fundamental para a inserção efetiva do Estado de Minas Gerais na sociedade da informação.

**“...o Governo de Minas, em consonância com o Programa de Governança Eletrônica, está promovendo ações para desenvolver um projeto de implantação de Modelo de Gestão de Segurança da Informação na Administração Pública do Poder Executivo Estadual.”**

**Renata Vilhena**

**Secretária-adjunta de Planejamento e Gestão do Governo do Estado de Minas Gerais**



# Criptografia na ficção

## Técnicas antigas e fantasias modernas

Luís Carlos Silva Eiras

A mais famosa mensagem secreta da ficção foi escrita na parede do palácio do rei Baltazar: “*Menê menê tequêl u-parsîn*”. E foi decifrada pelo profeta (e criptólogo) Daniel, conforme se lê no capítulo 5 do seu livro, e é sobre o breve futuro do rei – Baltazar morreu momentos depois da mensagem lida. Da Bíblia para cá, muitos são os exemplos de mensagens secretas em narrativas, já que boa parte da ficção conta a história de investigações e, com uma mensagem a ser decifrada, já se tem o principal da história.

É o que faz Edgar Allan Poe em *O Escaravelho de Ouro*, novela publicada em 1843. Conta como um pergaminho, descoberto numa praia, continha uma mensagem secreta e como ela foi decifrada, possibilitando que se achasse um tesouro de piratas. Allan Poe se concentra primeiro em explicar que, a partir de uma tabela de frequência, os caracteres sem sentido vão, aos poucos, revelando um texto – que, por sua vez, não faz o menor sentido! Então, Poe usa a imaginação para revelar o sentido desse texto e achar o tesouro. Uma proeza de dupla decifração.

Não era a primeira vez que Poe tocava no assunto. Em 1841, publicou num jornal que tinha recebido duas mensagens secretas de um certo W. B. Tyler, mas, apesar de ter decifrado mais de cem mensagens, estava sem tempo (!) para resolvê-las, deixando isso para os leitores. Essas mensagens

demoraram 150 anos para ser decifradas, a primeira, em 1992, por Terence Whalen, e, a segunda, em 2000, por Gil Broza, o que acabou com qualquer dúvida sobre quem era o tal W. B. Tyler. Allan Poe escreveu ainda o ensaio *Criptografia* (1842), uma prévia de *O Escaravelho de Ouro*.



Outro autor famoso que usa o assunto é Júlio Verne. Em *Matias Sandorf* (1885), a criptografia é feita através de uma tabela de três colunas de letra, sobre a qual se colocam cartões perfurados. As letras que ficam visíveis formam a mensagem. Com esse método, foi possível decifrar neste ano o manuscrito Voynich, 230 páginas de uma escrita incompreensível por mais de 5 séculos. Agora se sabe: o

manuscrito não faz mesmo sentido e trata-se de uma fraude.

Mesmo em romances mais recentes, são utilizadas criptografias antigas como no *O Nome da Rosa* (1980) e *O Pêndulo de Foucault* (1988), de Umberto Eco. O primeiro usa a substituição de palavras por símbolos, o segundo, o cifrário de Vigenère, conhecido desde o século XVI.

Carl Sagan, em *Contato* (1985), é que inventa algo complicado. Imagens da transmissão de TV das

Olimpíadas de Berlim, de 1936, foram capturadas por extraterrestres e reenviadas para a Terra. Só que, no meio das frequências da velha transmissão, havia mensagens para os terráqueos. Michael Crichton, em *Esfera* (1987), é mais modesto. Uma nave espacial encontrada no fundo do Oceano Pacífico envia uma seqüência de números, que vão aos poucos sendo reagrupados até formarem mensagens inteligíveis.

Mais recente, *Cryptonomicon*, de Neal Stephenson, de 1999, faz a ligação entre os decifradores dos códigos alemães da Segunda Guerra Mundial e os hackers atuais, para quem conseguir atravessar as suas 900 páginas de idas e vindas no tempo.

No cinema, também aparecem criptografias bem variadas, que tentam, às vezes, se aproximar da realidade. Não é o caso de *Quebra de Sigilo* (1992), onde Robert Redford vai atrás de uma caixa capaz de quebrar a senha de qualquer computador, já que a caixa sabe como funcionam os números primos<sup>1</sup>. Nem de *Código para o Inferno* (1998), onde Bruce Willis se envolve com um garoto autista que sabe ler códigos secretos, que custaram um bilhão de dólares para ser desenvolvidos. Muito menos é o caso de *A Senha* (2001), onde um hacker consegue digitar mais rápido do que um programa de segurança.

Mas é o caso de *Enigma* (2001). Dougray Scott faz um matemático mais ou menos baseado em Alan Turing e mostra como os ingleses decifraram os códigos secretos dos alemães utilizando o *Colossus*, o primeiro computador. (Mostra também, numa cena de bar, Mick Jagger, o produtor do filme.) Turing é o personagem principal da peça *Breaking The Code* (1987), de Hugh Whitmore, onde conta como ele e Churchill leram todas as mensagens secretas dos

nazistas, inclusive a localização do *Bismarck*, o que possibilitou seu afundamento em 1941<sup>2</sup>.

Já o filme *U-571* exagera na importância da captura de uma máquina Enigma num submarino alemão pelos americanos. Os poloneses conheciam o funcionamento da máquina desde o início dos anos 30 e repassaram esse conhecimento para os franceses e ingleses. Eles sabiam também que não era suficiente conhecer seu funcionamento para decifrar as mensagens codificadas. Porém, a versão

em DVD tem uma boa entrevista com David Kahn, autor do clássico *The Codebreakers* (1996), ainda não editado no Brasil.

Mas é em *Uma Mente Brilhante* (2001) que essa história de decifrar códigos secretos aparece em filme da maneira mais interessante. Russel Crowe faz o matemático John Nash, que era capaz de ler códigos secretos russos escondidos em notícias de jornais e revistas. Todos imaginários.

“... boa parte da ficção conta a história de investigações e, com uma mensagem a ser decifrada, já se tem o principal da história.”

## NOTAS

<sup>1</sup> Se você também sabe como funcionam os números primos, você pode ganhar um milhão de dólares. É só responder sobre a conjectura de Riemann para o Instituto Clay de Matemática do MIT. Mais informações em <http://www.claymath.org/millennium/>.

<sup>2</sup> O funcionamento do Enigma, do Colossus e de outros métodos citados aqui pode ser testado pelo leitor em <http://www.apprendre-en-ligne.net/crypto/>.

**Luís Carlos Silva Eiras**

Analista de Sistemas da Prodemge



# Certificação Digital:

## o fio de bigode eletrônico

Confiança e segurança. As bases históricas das relações, sejam elas comerciais ou não, sobrevivem intactas, ao longo do tempo, às mudanças culturais, sociais ou tecnológicas, embora agora marcadas pela impessoalidade. São fundamentos de grandes e pequenas operações, condições para que alianças se concretizem.

O velho "fio de bigode", a caderneta do armazém ou a palavra empenhada, atributos incontesteáveis de confiança, que vêm assegurando a confiabilidade das partes envolvidas em qualquer transação comercial, ganham, como tudo na era digital, a sua versão eletrônica.

Adaptado à consolidação da internet e ao crescimento desenfreado das operações feitas através da rede mundial de computadores, um novo recurso tecnológico passa a se integrar aos poucos à vida dos brasileiros: a certificação digital, que agrega aos documentos eletrônicos, inclusive aos e-mails, a garantia de sua autoria e autenticidade, imprimindo às operações eletrônicas segurança e confiabilidade.





instantaneidade que a tecnologia imprime às comunicações passou a exigir mecanismos que assegurem às empresas, sejam elas públicas ou privadas, e às pessoas, físicas ou jurídicas, pleno aproveitamento do potencial oferecido pela tecnologia da informação.

A certificação digital é um arquivo eletrônico que acompanha um documento assinado digitalmente, contendo informações que identificam a empresa ou a pessoa com quem se está tratando na rede. Um documento eletrônico com certificação digital tem, portanto, validade jurídica. Isso garante sua autenticidade de origem e autoria, integridade de conteúdo, confidencialidade e irretratabilidade, ou seja, que a transação, depois de efetuada, não possa ser negada por nenhuma das partes.

Além da segurança e velocidade na tramitação de documentos, a certificação digital transcende a questão de espaço, ao permitir, por exemplo, que um executivo possa assinar normalmente um documento juridicamente válido a partir de qualquer ponto geográfico e em qualquer horário, com o mesmo valor de um documento em papel. Viabiliza ainda a guarda e o arquivamento seguros de documentos - oficiais ou não - com a mesma validade do seu original em papel.

O diretor de Infra-Estrutura de Chaves Públicas do ITI - Instituto Nacional de Tecnologia da Informação - autarquia federal vinculada à Secretaria da Casa Civil da Presidência da República, Renato Martini, resume os benefícios do uso dessa tecnologia. Para ele, a certificação digital agrega aos serviços maior segurança, transparência, desmaterialização, redução do consumo e trânsito de papéis, contribuindo para a diminuição do custo Brasil. Do ponto de vista institucional e social, melhora a relação do Governo com o cidadão e abre possibilidades para oferta de mais serviços pela internet - o cidadão não precisa sair de casa para ter acesso a uma série de serviços, na medida em que esteja equipado para se identificar na rede.

A assinatura eletrônica não é, no entanto, a digitalização de uma assinatura, mas um complexo sistema de códigos. Para o advogado especialista em Direito Internacional e professor gaúcho Fabiano Menke, ex-procurador

geral do Instituto Nacional de Tecnologia da Informação, a assinatura digital é um meio de agregar confiança ao ambiente virtual, confirmando a importância da autoria e identificação principalmente para questões legais. A assinatura digital agrega à internet, segundo ele, o atributo da identificação: tem, portanto, os mesmos efeitos de uma assinatura manuscrita feita no papel.

Um certificado digital contém informações relativas a seu usuário: a codificação de sua assinatura (chave privada), nome e endereço de e-mail, identificação da Autoridade Certificadora, número de série, a assinatura digital e o período de validade do certificado, que pode ser de um ou dois anos.

A chave privada do usuário pode ser armazenada em seu microcomputador, ou ainda num smart card ou token, que são mídias portáteis, que permitem seu uso a partir de outras estações. O acesso às informações contidas em seus chips é feito por meio de uma senha pessoal, determinada pelo titular. O smart card assemelha-se a um cartão magnético, sendo necessário um aparelho leitor para seu funcionamento. Já o token assemelha-se a uma chave e requer a conexão à porta USB do computador. A segurança desses três recursos é garantida também por senha.

Quanto aos preços, podem ainda ser considerados altos. Segundo o presidente da CertiSign, uma das empresas certificadoras credenciadas pela ICP/Brasil – Infra-Estrutura de Chaves Públicas, Sérgio Kulikovsky, “a média é de R\$100,00 por certificado (com validade de um ano), considerado compatível com a capacidade do usuário”. Ele prevê que esse preço caia a médio prazo: “Naturalmente, na medida em que se aumenta a demanda, o preço cai, uma vez que é estabelecido em função da quantidade”. E conclui: “Se o serviço oferecido é bom, o preço se justifica pelo benefício que ele oferece”.

### **Chaves Públicas - a questão legal**

No Brasil, a exemplo do modelo adotado pela comunidade européia, a certificação digital pode ser

concedida a pessoas físicas e a pessoas jurídicas por diferentes autoridades certificadoras que, por sua vez, podem ser públicas ou privadas. O sistema oficial brasileiro de certificação digital baseia-se na ICP-Brasil – Infra-Estrutura de Chaves Públicas Brasileira, regulamentada pela Medida Provisória 2200-2, de agosto de 2001. Ela foi instituída para “garantir a autenticidade, a integridade, a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras”. O ITI é a Autoridade Certificadora Raiz da estrutura.

De acordo com a Medida Provisória, a organização da matéria é composta por uma autoridade gestora de políticas – o Comitê Gestor da ICP-Brasil – e pela cadeia de autoridades certificadoras, composta pela Autoridade Certificadora Raiz (AC-Raiz), pelas Autoridades Certificadoras (AC) e pelas Autoridades de Registro (AR). O Comitê Gestor é composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante dos ministérios da Justiça; da Fazenda; do Desenvolvimento, Indústria e Comércio Exterior; do Planejamento, Orçamento e Gestão; da Ciência e Tecnologia; da Casa Civil da Presidência da República e do Gabinete de Segurança Institucional da Presidência da República.

O Comitê Gestor estabeleceu o padrão tecnológico mínimo para emissão da certificação digital, e os pré-requisitos para que órgãos públicos ou privados se tornem autoridades certificadoras credenciadas. O sistema dá validade jurídica a documentos enviados por e-mail e a transações feitas pela internet que estejam com certificação. Atualmente, estão cadastradas pela ICP/Brasil para atuar como autoridades certificadoras as seguintes entidades: Presidência da República, Serpro, Serasa, CertiSign, Caixa Econômica Federal e Secretaria da Receita Federal.

O advogado Fabiano Menke comenta, em artigo sobre Interoperabilidade Aplicada à ICP, “o acerto da posição adotada pelo Brasil” na aprovação da

Medida Provisória: “Sem proibir que o mercado (aqui entendido como o conjunto dos agentes não estatais) implante soluções que possam vir a ser díspares no sentido de não direcionadas à coletividade, decidiu-se por fundar uma espinha dorsal normativa comum, um tronco ou, mais precisamente, uma árvore invertida, situando no topo (na raiz da árvore invertida) uma entidade de direito público, a autarquia federal Instituto Nacional de Tecnologia da Informação - ITI, com as atribuições principais de auditar, credenciar e fiscalizar as autoridades certificadoras, autoridades de registro e prestadores de serviços de suporte que integram a ICP-Brasil”.

O advogado, que é mestre em Direito Especial – Efeitos Jurídicos da Assinatura Digital –, comenta outros benefícios de uma estrutura nacional: “Havendo uma ICP mais abrangente, como são a brasileira e a alemã, torna-se bem mais viável e atraente a celebração de acordos internacionais de reconhecimento recíproco de certificados digitais, o que possibilitará transações eletrônicas internacionais mais seguras entre empresas e entre consumidores e empresas”.

Está em tramitação no Congresso Nacional o Projeto de Lei 7316/2002, que disciplina o uso de assinaturas eletrônicas e a prestação de serviços de certificação. A necessidade e urgência de aprovação dessa Lei são defendidas pelo diretor de Infra-Estrutura de Chaves Públicas do ITI, Renato Martini: “O maior mérito é institucionalizar uma estrutura que está funcionando operacionalmente. O Brasil vai ganhar uma Lei para disciplinar a questão”, afirma. “A Lei é flexível, pode ser alterada, ao contrário da Medida Provisória; pode sofrer emendas e se adaptar à evolução da sociedade. É muito importante uma Lei disciplinando a questão da certificação digital e da estrutura de chaves públicas”, garante. O Projeto de Lei tem como relator o deputado federal Jorge Bittar.

(Confira, nesta edição, na seção “Diálogo” - página 4 - entrevista com o advogado-geral do Estado de Minas Gerais, José Bonifácio Borges de Andrada, abordando, dentre outros aspectos, a questão legal da certificação digital no País).

Pensar nos benefícios da Certificação Digital significa, em resumo, pressupor a falta de riscos no ambiente vir-



tual, uma vez que a tecnologia utilizada no processo coíbe a ação de hackers na adulteração ou interceptação de documentos ou mensagens eletrônicas. Como um documento selado, evita-se, inclusive, a leitura de conteúdos por pessoas não autorizadas.

Facilidades como essas têm ampliado de forma expressiva o seu uso: segundo Sérgio Kulikovsky, há hoje aproximadamente 200 mil certificados emitidos em todo o território nacional, a maior parte para pessoas físicas, em uso profissional. “O número de certificados tem crescido muito”, avalia. “Neste ano, registramos cerca de 50% de crescimento em relação ao ano passado.” Para o ano que vem, a expectativa é de que esse número cresça ainda mais. “A previsão é de que teremos pelo menos 1 milhão de certificados emitidos em 2005.”

Esse crescimento se justifica, para Sérgio Kulikovsky, pelos investimentos que têm sido feitos na tecnologia que viabiliza seu uso. “A tendência é um rápido crescimento daqui para a frente; o mercado necessitava de uma série de requisitos de infra-estrutura, e têm sido feitas muitas implementações, que abrem agora uma boa perspectiva.”

“A popularização da certificação digital é fundamental para garantir a privacidade e os novos direitos na sociedade em rede”, afirma o diretor-presidente do ITI, Sérgio Amadeu da Silveira. “É, também, uma forma de dar mais segurança às transações eletrônicas. Atualmente, há vários projetos para dar mais segurança aos dados que transitam na rede. Podemos citar, como exemplo, uma política de divulgação, com utilização de mídia dirigida, eventos, entre outros, com o objetivo de tornar essa tecnologia mais conhecida.”

Em sua experiência à frente da CertiSign, Kulikovsky afirma que as resistências que se anunciavam no início do processo, em grande parte atribuídas à cultura do uso do papel, aos poucos vão dando lugar à aceitação de um recurso que tem se mostrado seguro. “Havia também o desafio da tecnologia, com relação à segurança e avaliação da possibilidade de risco” – lembra. “Mas, cada vez mais, as pessoas

vêm que esse tipo de questão não procede, elas vão se convencendo de que o recurso é, de fato, bom. Que vale a pena, desde que cercado das devidas precauções.”

O leque de empresas usuárias, representantes dos mais variados setores, se abre com a consolidação da tecnologia, contemplando principalmente aqueles que envolvem públicos de relacionamento numerosos, como é o caso das empresas públicas e do sistema bancário. O Sistema de Pagamentos Brasileiro, por exemplo, que movimenta diariamente milhões de reais entre os bancos, emprega de forma efetiva a certificação digital.

Da mesma forma, a Receita Federal se prepara para tornar ainda mais segura a relação com os contribuintes: brevemente, seus 25 mil servidores estarão utilizando certificados digitais, garantindo de forma mais eficaz o sigilo fiscal. A Receita investe também na segurança da Declaração de Imposto de Renda Retido na Fonte, trabalhando em conjunto com o ITI e bancos públicos e privados no projeto de emissão dos CPFs eletrônicos - E-CPF, que deverá contemplar todos os correntistas do País, substituindo o CPF em papel pelo eletrônico a médio e longo prazos. *(Detalhes na página 32).*

Governos estaduais descobrem nessa tecnologia a solução não só para a troca de documentos entre membros do alto escalão - no envio de conteúdos formatados eletronicamente para publicação em seus diários oficiais e tramitação burocrática de projetos de Lei -, mas, também, envolvendo contribuintes, como é o caso do Governo de Pernambuco, estado brasileiro pioneiro na adoção da tecnologia.

A Secretaria da Fazenda do Estado disponibilizou um conjunto de serviços pela internet, permitindo que os contribuintes inscritos sob regime normal de apuração cumpram com suas obrigações relativas às informações econômico-fiscais, aos benefícios fiscais do Prodepe - Programa de Desenvolvimento de Pernambuco - e à escrita fiscal mensal.

Na área jurídica, que trata com grandes volumes de papel na tramitação de documentos, a adoção da

certificação digital é recebida com empenho e bons resultados. O Tribunal de Justiça do Rio Grande do Sul já adota um sistema de informatização de sessões que permite que desembargadores redijam votos em seus gabinetes, compartilhem textos e emitam acórdãos com assinatura digital para publicação em tempo real na internet. No Rio de Janeiro, o Tribunal de Justiça implementa sistema para aumentar a segurança no uso de documentos resultantes de atos notariais.

Outro exemplo de sucesso é o Peticionamento Eletrônico adotado pelo Tribunal Regional de Trabalho/ 4ª Região, no Rio Grande do Sul, que tem proporcionado, desde junho de 2004, ganhos importantes para advogados e para o sistema. Segundo o diretor da Secretaria de Informática da entidade, Eduardo Kenzi Antonini, não há ainda mensuração matemática desses resultados, devido ao curto espaço de tempo desde sua implantação, mas o ganho em segurança é evidente, e a redução de custos para advogados de todo o Estado é drástica: “Não é necessário comparecer pessoalmente para entrega das petições; a economia de tempo e dinheiro com deslocamentos e hospedagens é expressiva. É importante destacar o aspecto da segurança da informação, pois não há extravio de documentos e garante-se a autenticidade e o não-repúdio, premissas que, num Tribunal, são essenciais”.

O serviço de Peticionamento Eletrônico ganha agora proporções nacionais, com o projeto E-Doc – Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos da Justiça do Trabalho –, que está em desenvolvimento, sob coordenação do TRT 4ª Região (*Detalhes na seção Benchmarking, página 33*).

O emprego da certificação digital ganha terreno também no comércio eletrônico, garantindo segurança aos compradores virtuais de produtos em sites seguros, identificados através da imagem de um cadeado; e nas áreas médica e odontológica, em prontuários virtuais.

Sérgio Kulikovsky identifica a generalização do uso da certificação, que já extrapola as entidades detentoras de grandes públicos de relacionamento, como bancos e seguradoras. Segundo ele, o Estado é um dos grandes usuários, mas profissionais liberais também já reconhe-



cem a importância da segurança em seus relacionamentos pela internet.

Opinião semelhante tem o diretor de Infra-Estrutura de Chaves Públicas do Instituto Nacional de Tecnologia da Informação, Renato Martini. Segundo ele, o poder público, através das aplicações do Governo Eletrônico, começa a se aproximar de um sistema de certificação digital. As máquinas financeira e bancária se apresentam mais organizadas e adiantadas que os governos. “Isso não é por acaso” – explica. “Reflete a conjuntura que criou a ICP, em 2001.”

Renato Martini explica: “O sistema financeiro tradicionalmente investe em tecnologia; portanto, para o setor, isso não é novidade. Quando se trata de usar a tecnologia para implementar segurança, isso também não é novidade. Já com as aplicações do Governo Eletrônico, não é tão fácil. São instituições que trabalham com tempos diferentes”.

Para Sérgio Kulikovski, um dos aspectos mais importantes de todo o processo, no momento, refere-se às perspectivas que a construção de uma infraestrutura tecnológica satisfatória viabiliza. Ele defende a opinião de que “o principal é poder oferecer mais serviços, para mais gente, de maneira menos burocrática e mais transparente”.

As restrições impostas pela falta de segurança - característica da rede mundial de computadores - limitaram, ao longo do tempo, a oferta de serviços, que acabaram por se perpetuar no papel. Sérgio Kulikovsky defende que o foco das empresas, a partir desse momento, deve estar nas possibilidades de ampliação de seu leque de produtos e serviços com base na segurança que a certificação agrega a quaisquer operações eletrônicas.

Para ele, “o grande desafio da certificação, agora, está na criação de aplicações úteis”. Ou seja, “pensar em quem vai usar, como e por que vai usar. O foco deve, portanto, ser deslocado da tecnologia para sua aplicação inteligente e útil, abandonando mitos e focalizando o usuário”.

## **Inclusão Digital - Inclusão Social**

Se a certificação digital representa a possibilidade de oferta de um número maior de novos serviços por um universo mais abrangente de empresas, o mesmo pode ser dito da ampliação dos usuários potenciais num segmento já tão elitizado? Na opinião do diretor do ITI, Renato Martini, sim. “Atualmente, não se pode falar de inclusão social sem associar a idéia da inclusão digital”, explica. “A tecnologia está presente fortemente em todos os setores e uma das ações políticas do Governo Federal é a popularização desse serviço. Todo cidadão que tiver uma conta bancária terá acesso. Se você populariza uma tecnologia, você promove a inclusão digital. A participação do cidadão brasileiro no uso de uma tecnologia de ponta promove naturalmente a inclusão social.”

A transparência que a certificação viabiliza para usuários detentores de um certificado é considerada, pelo presidente da CertiSign, um elemento de inclusão. “O cidadão passa a ter mais acesso ao que está acontecendo, pode acompanhar e até mesmo fiscalizar os serviços que são oferecidos. Isso significa que mais gente pode ter acesso a mais informações”, afirma. Com relação à indisponibilidade de microcomputadores em domicílios de baixa renda, Kulikovsky argumenta: “Não é necessário que você tenha um computador. Com o smart card ou token (mídias portáteis), o cidadão pode ter acesso a serviços e informações a partir de qualquer lugar, de qualquer computador. Você é você em qualquer lugar onde esteja. Você deixa de ser uma senha e passa a ser você de fato; passa a ser parte do processo”.

## **Interoperabilidade**

Garantir que todos os equipamentos que compõem a infra-estrutura da certificação digital no Brasil se comuniquem, independente do modelo, fabricante ou procedência, tem sido uma preocupação das autoridades envolvidas no processo. Para o advogado Fabiano Menke, “a interoperabilidade é um atributo necessário a qualquer infra-estrutura que

pretenda atingir a coletividade”.

Na sua opinião, em artigo sobre o tema, “a idéia que influenciou a criação da ICP-Brasil foi justamente a de construir uma infra-estrutura para a coletividade, para toda a sociedade, tornando mais facilitada a comunicação entre os titulares de certificados digitais”. Ele defende a necessidade de padronização, “a fim de que, na prática, se tenha a possibilidade de assinar digitalmente, bem como verificar as assinaturas digitais a partir de qualquer equipamento”. (*Leia artigo de Fabiano Menke sobre o assunto na página 39*).

Nesse sentido, o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira aprovou, no dia 21 de outubro, através da Resolução nº 36, o regulamento para homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil. A condução do processo será feita pela Autoridade Certificadora Raiz da ICP-Brasil, o Instituto Nacional de Tecnologia da Informação - ITI, e contempla mídias como tokens criptográficos e smart cards, sistemas como de assinatura eletrônica, de autenticação de assinatura, de autoridades certificadoras e de registro, e equipamentos como os de HSM, sincronismo e carimbo de tempo, entre outros.

Segundo o diretor-presidente do ITI, Sérgio Amadeu da Silveira, “a implementação de um laboratório que checará e homologará os dispositivos de segurança, como smart cards, que suportam os certificados, é uma iniciativa relevante. Já que, a partir dessa checagem, teremos certeza, seja qual for o fabricante do dispositivo, de que ele será interoperável, ou seja, aceito em todos os sistemas. Essa iniciativa reduzirá os custos dos certificados, facilitando a sua utilização em escala. O Governo, também, tem feito um esforço de utilizar essa tecnologia como forma de reduzir o trâmite de papéis e dar rapidez aos processos”.

O estabelecimento de padrões e especificações técnicas mínimas garantirá, portanto, a sua interoperabilidade e a confiabilidade dos recursos de segurança da informação. De acordo com a Resolução, os produtos homologados terão um laudo de conformidade emitido e utilizarão o selo de homologação e seu correspondente número de identificação. Para isso, já foi inaugurado, em novembro, o primeiro Laboratório de Ensaios e Auditoria –

LEA, em São Paulo, numa parceria do ITI com o Laboratório de Sistemas Integráveis – LSI da Escola Politécnica da USP. O LEA será responsável pela homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil.

### **Chaves Públicas**

O sistema de chaves públicas prevê a certificação através de duas chaves, uma chave privada – do seu proprietário, o remetente – utilizada para assinar o documento; e uma chave pública, de conhecimento geral, que validará a assinatura, consolidadas ambas num certificado digital.

O que garante segurança ao processo é justamente a autoridade certificadora, uma terceira entidade presente no processo, que atesta para o destinatário que o remetente é quem de fato assina o documento. O processo de emissão de um certificado pressupõe o reconhecimento pessoal do interessado em ter seu certificado pela entidade certificadora. Funciona, em outras palavras, como uma assinatura reconhecida em cartório pelo tabelião, que assegura que determinada assinatura pertence de fato àquela pessoa.

A tecnologia adotada é a criptografia assimétrica. Isso quer dizer que é impossível identificar o código de uma das chaves a partir da outra. Outra característica é o fato de uma chave desempenhar exatamente função inversa à outra: uma delas – a privada – é usada para assinar o documento; a outra, a chave pública, é utilizada para reconhecer a autenticidade da assinatura.

A criptografia assimétrica se distingue da criptografia simétrica: neste caso, ambos – remetente e destinatário – conhecem o algoritmo utilizado para criptografar a mensagem, o que a torna menos segura.

As chaves garantem não só a autenticidade da assinatura, mas também a comunicação segura para troca de documentos e mensagens. Um dispositivo, o “algoritmo de hash”, é capaz de acusar qualquer

interferência na mensagem em seu trânsito entre o remetente e o destinatário.

### **Assinatura Eletrônica x Assinatura Digital**

O professor Fabiano Menke define de forma esclarecedora a diferença básica entre a assinatura eletrônica e a assinatura digital. Insere-se na primeira categoria qualquer meio para identificar o remetente de uma mensagem, como a assinatura escaneada ou digitalizada. Mesmo que a ela sejam associados outros atributos - como digitais, íris, voz - é facilmente editável, estando portanto mais sujeita a fraudes.

Já a assinatura digital é algo mais, por associar inequivocamente uma pessoa a um documento, um código exclusivo a uma pessoa. Baseia-se na criptografia assimétrica – uma parte é privada e outra é pública –, ao contrário da criptografia simétrica, em que ambas as partes compartilham um código. Pressupõe ainda uma autoridade certificadora.

### **Governo Mineiro Adota Certificação Digital**

A administração pública em Minas conta com os benefícios da tramitação de documentos e informações pela internet de forma segura, através da tecnologia de certificação digital. A Companhia de Tecnologia da Informação de Minas Gerais - Prodemge - é a Autoridade Certificadora em Minas, coordenando um dos principais projetos previstos no Programa de Governança Eletrônica do Governo do Estado.

A adoção da tecnologia no Governo de Minas foi feita dentro dos parâmetros estabelecidos pela ICP-Brasil, portanto, orientada por padrões internacionais, que colocam a administração pública mineira em condições de se relacionar virtualmente com entidades de todo o mundo.

Para emitir os certificados, a Prodemge adequou sua infra-estrutura às exigências da ICP-Brasil. Foi feito processo de licitação para contratação de uma autoridade certificadora denominada de primeiro nível



– a CertiSign foi a vencedora - que hospeda em suas instalações os utilitários e o ambiente de segurança necessários, eliminando, num primeiro momento, a necessidade de grandes investimentos para montagem da estrutura. A equipe técnica da Prodemge também desenvolveu as aplicações de suporte ao serviço.

Para o diretor do ITI, Renato Martini, a Prodemge reflete hoje a aplicação da certificação digital no serviço público: “A empresa inteligentemente escolheu um dos cenários possíveis dentro dos parâmetros do ICP, ao aproveitar uma estrutura já existente, que custou grandes investimentos ao Governo e à sociedade”. Ela poderá, como AC, cadastrar, fazer a identificação física para emissão do certificado e ter o certificado para usar em seus procedimentos dentro do Governo. “Em um outro momento, a Prodemge poderá optar por evoluir para atuar como autoridade certificadora de primeiro nível”, explica Martini. “Nesse caso, é necessária a montagem da estrutura que exige grandes investimentos, como a sala-cofre e uma estrutura complexa de criptografia. Há cenários diferentes, a regulamentação da ICP é bastante flexível, oferecendo várias possibilidades.”

A adoção da certificação digital pelo governo mineiro representa um importante passo na modernização do Estado, ao eliminar de forma substancial a necessidade da tramitação de papéis.

Os primeiros projetos de certificação digital desenvolvidos são para a Junta Comercial do Estado de Minas Gerais – Jucemg – para envio eletrônico de livros mercantis, com significativa redução da tramitação de papéis e agilização do processo. Outra aplicação é da Secretaria de Estado de Planejamento e Gestão, e abrange todo o processo de tramitação de atos normativos do Governo provenientes da Secretaria, utilizando ferramenta de workflow. A Secretaria de Governo do Estado passa a contar com o Sistema Integrado de Processamento de Atos - SIPA -, destinado aos atos de provimento de cargos comissionados. A assinatura digital para responsáveis por esses atos representa também mais agilidade e economia na tramitação de papéis.

Outras aplicações que se beneficiarão de forma efetiva do serviço são a tramitação de informações e documen-

tos da Secretaria da Fazenda com os contribuintes do ICMS; a gestão eletrônica de documentos da Junta Comercial, que representa grandes volumes de papel; o relacionamento da Secretaria de Planejamento e Gestão com os fornecedores de serviços e produtos para o Estado; o envio de documentos oficiais para publicação pela Imprensa Oficial do Estado e a identificação segura de usuários dos sistemas corporativos do Estado, entre várias outras.

## **Empresas públicas estaduais e a certificação digital**

O Instituto Nacional de Tecnologia da Informação - ITI vem trabalhando com as empresas da ABEP – Associação Brasileira de Empresas Estaduais de Processamento de Dados-, a fim de consolidar a tecnologia junto aos governos estaduais. Segundo o diretor do Instituto, Renato Martini, já foram promovidos encontros em Brasília, com o presidente do Conselho da entidade, Marcos Vinícius Ferreira Mazoni, e com os presidentes das empresas estaduais de processamento de dados em Florianópolis, na última edição do Secop – Seminário Nacional de Informática Pública.

O ITI conduz um projeto de comunicação que visa a esclarecer o tema para as áreas públicas estadual e municipal. “Entendemos que a entrada da certificação digital para o serviço público é através das empresas estaduais de informática e chamamos a Abep para ser protagonista nesse processo, através de uma ação coordenada que contribua para a institucionalização do projeto.” Martini argumenta que é importante que as empresas públicas se organizem para ter um padrão, se coordenem e desenvolvam um projeto coletivo.

Para ele, trata-se de uma tecnologia complexa. “Daí a importância de explicar ao gestor público o seu funcionamento e benefícios. Estamos fazendo contato com os profissionais da área pública. Pernambuco tem hoje seus procedimentos fazendários baseados na certificação digital. Foi o Estado que saiu na frente. Há também boas iniciativas no Poder Judiciário. Mas é possível perceber um

desnível no conhecimento e aplicação da certificação digital entre os estados – alguns muito avançados, outros, não.”

O projeto do ITI busca justamente levar ao gestor público esse conhecimento. “Estamos elaborando guias, manuais, com conteúdo esclarecedor e texto de fácil entendimento.” O material será produzido pela Universidade Federal de Santa Catarina, que tem convênio com o ITI.

## **Dicas do ITI para maior segurança na utilização da certificação digital**

(fonte: site do ITI)

Primeiramente, deve-se lembrar que o certificado digital representa a “identidade” da pessoa no mundo virtual. Assim, é necessária a adoção de alguns cuidados para se evitar que outra pessoa possa praticar negócios jurídicos, acessar páginas na internet e realizar transações bancárias em nome do titular do certificado. Recomendações para o uso de um certificado digital:

- a senha de acesso da chave privada e a própria chave privada não devem ser compartilhadas com ninguém;
- caso o computador onde foi gerado o par de chaves criptográficas seja compartilhado com diversos usuários, não é recomendável o armazenamento da chave privada no disco rígido, pois todos os usuários terão acesso a ela, sendo melhor o armazenamento em disquete, smart card ou token;
- caso a chave privada esteja armazenada no disco rígido de algum computador, deve-se protegê-lo de acesso não-autorizado, mantendo-o fisicamente seguro. Nunca deixe a sala aberta quando for necessário sair e deixar o computador ligado. Utilize também um protetor de tela com senha. Cuidado com os vírus de computador, eles podem danificar sua chave privada;
- caso o software de geração do par de chaves permita optar entre ter ou não uma senha para prote-



ger a chave privada, recomenda-se a escolha pelo acesso por meio de senha. Não usar uma senha significa que qualquer pessoa que tiver acesso ao computador poderá se passar pelo titular da chave privada, assinando contratos e movimentando contas bancárias. Em geral, é bem mais fácil usar uma senha do que proteger um computador fisicamente;

- utilize uma senha longa, com várias palavras, uma vez que existem programas com a função de desvendar senhas. Deve-se evitar o uso de dados pessoais como nome de cônjuge ou de filhos, datas de aniversários, endereços, telefones ou outros elementos relacionados com a própria pessoa. A senha nunca deve ser anotada, sendo recomendável sua memorização.

## Como verificar uma assinatura digital?

Fonte: site da CertiSign

**Antes de confiar no conteúdo de um e-mail assinado digitalmente, você precisa verificar se o certificado utilizado para assiná-lo é legítimo. Nesse caso, a assinatura é verdadeira e você pode confiar no conteúdo da mensagem que recebeu, pois ela realmente foi enviada pela pessoa ou empresa que a está assinando.**

**Não ter esse cuidado pode significar confiar numa mensagem falsa, fraudada, em nome da pessoa ou empresa que a está assinando. Por isso, é importante verificar sempre a validade da assinatura digital antes de confiar nos e-mails e newsletters que você recebe.**

**Certificado válido significa assinatura verdadeira.**

**O procedimento de verificação é diferente para cada programa de e-mail.**

## Webmail

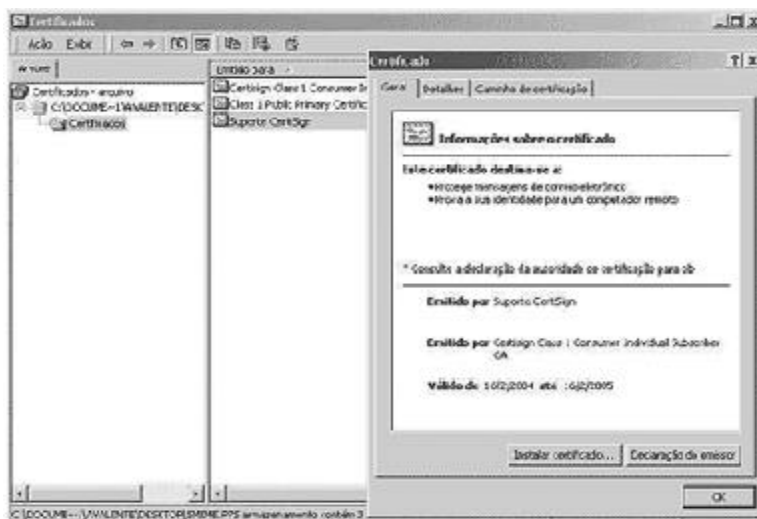
Quando recebemos um e-mail assinado digitalmente através de um webmail, o mesmo entende que a assinatura digital é um mero arquivo anexo (Smime.p7s) conforme a imagem abaixo:



Para poder verificar essa assinatura, você pode clicar no arquivo anexo e salvar o mesmo em sua área de trabalho.

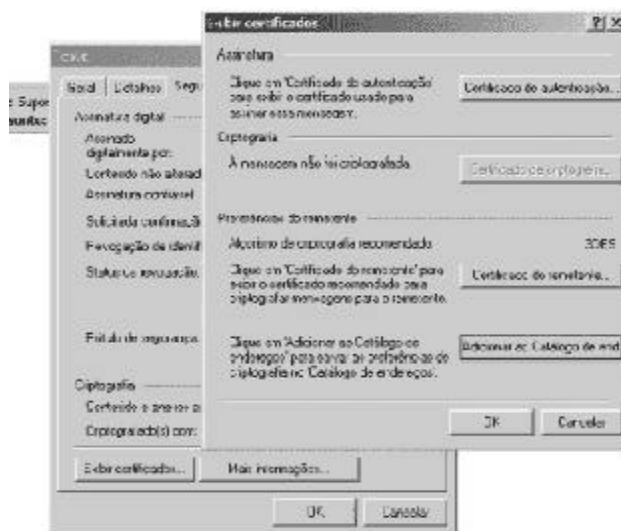
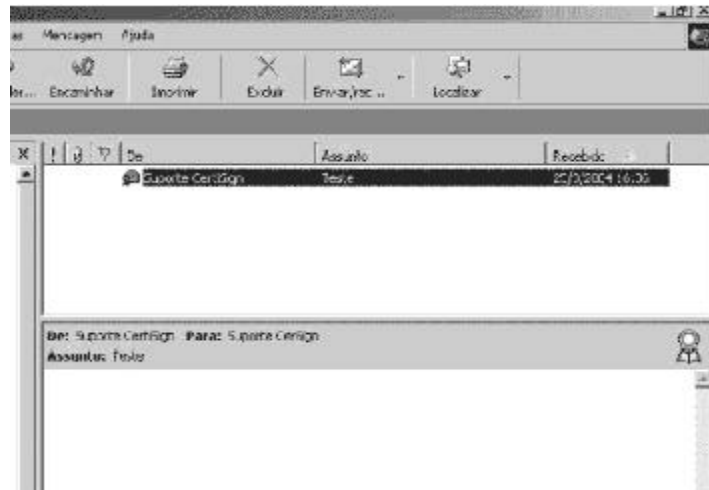


Após ter salvo o arquivo, você poderá dar um duplo clique no mesmo e verificar a assinatura digital que foi utilizada para assinar o e-mail que lhe foi enviado.



## Outlook

Ao receber um e-mail assinado, você irá visualizar uma chancela em vermelho no e-mail recebido.



Para verificar a assinatura do emissor, você deve clicar na mesma e, em seguida, nas opções "Exibir certificados" - "Certificado de autenticação".

Em seguida, lhe será mostrado o certificado digital que foi utilizado para assinar a mensagem.



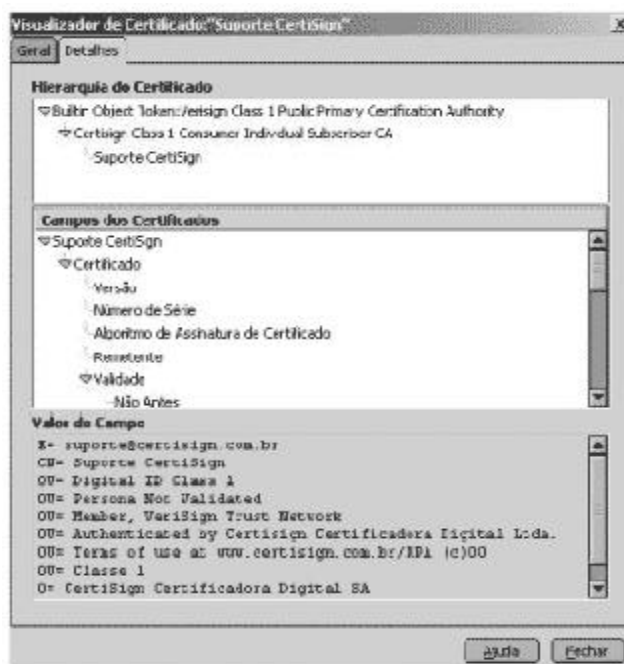
## Netscape

Ao receber um e-mail assinado utilizando o NetScape, você poderá visualizar uma “caneta” no cabeçalho da mensagem, representando que a mesma foi assinada digitalmente.



Para que você possa verificar a assinatura digital contida na mensagem, você deve clicar duas vezes neste ícone “Caneta” que a mesma irá lhe mostrar os dados referentes à certificação digital.

Para que você consiga todas as informações referentes a este certificado, você deverá clicar em “Exibir Certificado de Assinatura”.





## Glossário

**Autenticidade:** garantia de que a mensagem foi enviada por um remetente determinado e de que não é possível que outra pessoa se passe por ele.

**Autoridade Certificadora:** entidade autorizada a emitir certificados que vinculem uma determinada chave pública ao seu titular. Tem ainda outras atribuições, entre elas suspender, renovar ou revogar certificados digitais e emitir listas de certificados revogados.

**Confidencialidade:** atributo da mensagem protegida que garante que, após enviada, só será lida pelo destinatário e mais ninguém.

**Criptografia:** ramo das ciências exatas que tem como objetivo escrever em cifras. Trata-se de um conjunto de operações matemáticas que transformam um conteúdo em um texto cifrado.

**Garantia de Autoria:** presunção de que a mensagem é de fato assinada pela pessoa que se identifica.

**Interoperabilidade:** é pressuposto de uma infra-estrutura e pode ser definida como a capacidade que possuem os aparelhos e equipamentos que dela fazem parte de comunicarem-se entre si, independentemente de sua procedência ou de seu fabricante. (Fabiano Menke)

**Integridade:** garantia de que a mensagem que chega ao destinatário é exatamente a mesma que saiu do remetente, não tendo sofrido qualquer alteração em nenhuma de suas partes.

**Não-repúdio:** garantia de que o titular do certificado e autor da mensagem não pode negar a autoria de determinado documento. Numa situação assim, será dele o ônus de comprovar que seu certificado foi utilizado indevidamente.

**PKI:** tradução da expressão inglesa Public-Key Infrastructure - Infra-Estrutura de Chaves Públicas

**Token e smart card:** são hardwares portáteis que funcionam como mídias armazenadoras. Em seus chips, são armazenadas as chaves privadas dos usuários.

### Saiba Mais

---

Instituto Nacional de Tecnologia da Informação  
[www.iti.br](http://www.iti.br)

---

Infra-Estrutura de Chaves Públicas  
[www.icpbrasil.org](http://www.icpbrasil.org)

---

Companhia de Tecnologia da Informação do Estado  
de Minas Gerais  
[www.prodemge.mg.gov.br](http://www.prodemge.mg.gov.br)

---

CertiSign  
[www.certisign.com.br](http://www.certisign.com.br)

---

Tribunal Regional do Trabalho 4ª Região  
[www.trt4.gov.br](http://www.trt4.gov.br)

---

Módulo Security  
[www.modulo.com.br](http://www.modulo.com.br)



**Embora ainda em fase de consolidação no País, o uso da certificação digital ganha espaço em importantes setores da prestação de serviços públicos.**

**A seção Benchmarking mostra dois exemplos de projetos abrangentes e suas perspectivas para um número considerável de cidadãos brasileiros.**

## Receita Federal



Os 25 mil funcionários da Receita Federal, em todo o País, já se integram à crescente parcela de usuários da certificação digital. O órgão investe ainda na adoção dessa tecnologia para os contribuintes, ampliando o leque de serviços oferecidos pela internet, através do e-CPF ou CPF eletrônico, certificados digitais emitidos com a chancela do ICP-Brasil e que viabilizarão outro importante projeto: o Serviço Interativo de Atendimento Virtual, através do qual o contribuinte terá acesso, pelo computador, a serviços prestados atualmente apenas de forma presencial.

O projeto é conduzido em parceria com o ITI e bancos públicos e privados, para emissão de CPFs eletrônicos, que substituirão, a médio e longo prazos, o CPF em papel. As instituições bancárias deverão emitir um smart card contendo o certificado digital do cliente, com chancela da ICP-Brasil e o número de CPF do correntista. Esse talvez seja o mais

abrangente projeto em andamento no País, considerando-se o número de correntistas de bancos e a capilaridade das instituições bancárias.

Segundo o chefe da Divisão de Segurança da Informação da Receita Federal, Ariosto de Souza Júnior, a adoção da tecnologia para os funcionários e para os públicos de relacionamento da instituição se deve principalmente à consolidação da internet como canal de comunicação com o contribuinte: "Grande parte das informações com as quais lidamos são protegidas por sigilo fiscal, o que torna restrito o atendimento que podemos prestar se não tivermos a certeza de que o autor da demanda é efetivamente o contribuinte", explica.

Para ele, a certificação digital trará maior comodidade ao contribuinte, agilizará o atendimento aos processos e agregará maior segurança, consolidando, por

exemplo, um dos serviços importantes da Receita que é a entrega das declarações do Imposto de Renda: "Sem adotarmos a certificação digital, podemos receber as declarações via internet, mas alguns problemas que poderiam ser resolvidos remotamente acabam demandando o atendimento presencial, gerando desnecessárias filas nas delegacias da Receita".

Ele explica ainda como a tecnologia agregará agilidade ao processo: "Se recebemos um número cada vez maior de declarações via internet, a tendência é a Receita começar a dar encaminhamento aos processos todos de forma digital. Assim, por exemplo, quando um fiscal for analisar um processo, ele poderá assiná-lo eletronicamente com o seu e-CPF e aquele ato terá validade jurídica. A medida traz segurança aos sistemas informatizados da instituição e mais conforto também aos funcionários que, pelos métodos

tradicionais, têm que lembrar várias senhas para acesso a diferentes sistemas da Receita.

Ariosto de Souza Júnior lembra o processo de utilização da internet para oferta de produtos da Receita, que teve início em 1996, quando foram disponibilizadas somente a legislação tributária, informações de comércio exterior e trocas de informações com o contribuinte via correio eletrônico: “Em 97, a Receita disponibilizou o Recetanet, que é usado por 96% dos contribuintes brasileiros. Em 2004, o site da Receita registrou um total de 130 milhões de acessos e a entrega de 32 milhões de declarações. O serviço, que antes era utilizado apenas para a entrega das decla-

rações, já ampliou o atendimento a mais 120 outros documentos. Começamos então a disponibilizar serviços de consulta a aplicações, como a consulta à irregularidade fiscal e certidão negativa. Posteriormente, desenvolvemos aplicações para envio de dados como a declaração de isento, entre outras”.

A adesão dos usuários impôs, segundo Souza, a necessidade da implantação de novos recursos: “Avançamos até o limiar do que poderia ser oferecido sem ferir o sigilo fiscal. Como grande parte dos dados armazenados na Receita são protegidos por sigilo fiscal, chegamos no limite do que poderíamos fornecer sem a identificação do contribuinte”.

O processo de implantação da certificação digital passou pela aquisição de 27.500 smart cards, em fevereiro deste ano. Foram montados dois laboratórios de testes – um em Belo Horizonte, outro em Brasília –, além de um projeto piloto na Delegacia da Receita Federal em Contagem (MG). O projeto abrange 567 unidades da Receita Federal em todo o País.

“Usamos todo esse arranjo” – explica Ariosto Souza – “porque a Receita não quer aumentar o volume de atendimentos de balcão. Todo esse processo é para reduzir o atendimento presencial e facilitar a relação do contribuinte com a Receita”.



## **Tribunal Regional do Trabalho 4ª Região** **RIO GRANDE DO SUL**

No Rio Grande do Sul, o Tribunal Regional do Trabalho – 4ª Região implementou o primeiro sistema de Peticionamento Eletrônico do País, com adoção da certificação digital.

O serviço permite o envio eletrônico de petições através da internet, sem a necessidade da apresentação posterior dos ori-

ginais. A segurança da transação é garantida pela assinatura digital com utilização de certificados emitidos pela ICP-Brasil, que possuem validade jurídica de acordo com a Medida Provisória 2200-2.

Segundo o diretor da Secretaria de Informática do TRT, Eduardo

Kenzi Antonini, o projeto piloto foi desenvolvido com 20 advogados em dezembro de 2003 e, já em maio de 2004, o serviço foi ampliado para todos os interessados. Nos primeiros cinco meses do Peticionamento Eletrônico, cerca de 200 dos 8 mil advogados cadastrados no TRT4 já haviam adotado essa forma de trabalho.

Embora o pequeno tempo de uso do serviço não permita ainda medir com exatidão os seus resultados, o ganho em segurança e a redução de custos para advogados de todo o Estado é evidente. As vantagens se estendem também ao jurisdicionado, que ganha em rapidez e segurança; e ao sistema do judiciário, que ficou mais seguro - não há extravio de documentos -, ágil e simples. A autenticidade e o não-repúdio são, afinal, premissas essenciais num Tribunal.

### **Como funciona**

O TRT4 permite o envio de petições ao Tribunal e a todas as Varas do Trabalho da 4ª Região. Não estão contempladas no serviço as petições iniciais de 1ª instância e/ou seus aditamentos.

Em primeiro lugar, o usuário deve adquirir um certificado digital de qualquer entidade credenciada à ICP-Brasil. Para efetivar seu cadastro, é só acessar um formulário na internet e preencher os dados requisitados. No site do Tribunal, é possível fazer o download do Assinador Eletrônico; uma vez instalado no computador do usuário, o programa deverá ser usado para assinar eletronicamente suas petições, antes de enviá-las ao TRT.

Os arquivos são criptografados durante o envio. Ao receber a petição enviada eletronicamente,

o Tribunal analisa o arquivo recebido, verificando a validade da assinatura digital e se ela pertence efetivamente à petição enviada; consulta a data e a hora do recebimento junto ao Observatório Nacional; e gera um recibo da petição, que poderá ser impresso ou armazenado pelo advogado.

### **Projeto E-Doc**

O serviço de Peticionamento Eletrônico ganha agora proporções nacionais, com o projeto E-Doc – Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos da Justiça do Trabalho –, que está em desenvolvimento, a cargo do Grupo de Planejamento da Informatização da Justiça do Trabalho, coordenado pelo TRT da 4ª Região.

O objetivo é disponibilizar, através de infra-estrutura distribuída nos tribunais que compõem a Justiça do Trabalho, um sistema de envio e recebimento eletrônico de documentos aos Tribunais Regionais e ao Tribunal Superior do Trabalho. Da mesma forma que o Peticionamento Eletrônico do TRT4, será exigido o uso de certificados digitais emitidos pela ICP-Brasil, garantindo validade jurídica ao serviço.

Quando implantado, o E-Doc agregará ao sistema da Justiça do Trabalho mais agilidade e desburocratização, redução de custos e integração dos tribunais.

## Certificação Digital: o fim dos Cartórios?

**José Eisenberg**



A certificação digital – a atribuição de valor jurídico, através de criptografias personalizadas, para assinaturas enviadas através da rede mundial de computadores – apresenta um desafio instigante para o futuro da burocracia pública e privada, tal qual ela se conformou ao longo da história do Brasil. O nosso sistema jurídico, herdeiro do sistema centralizado português e sua estrutura oligárquica de

certificação de assinaturas em papel, em particular no Direito Civil, distribui a autoridade pública de certificação no mundo privado através de um sistema de cartórios, funcional e geograficamente atribuído, onde ainda funcionam antigas instituições de parentesco na reprodução do exercício daquela autoridade.

Para a economia, os cartórios representam simultaneamente custos de transação, a serem devidamente incluídos na formação de preços, e segurança para essas mesmas transações, em caso de litígios. Para o Direito, eles são entidades privadas investidas de autoridade pública cuja certificação confere validade a um documento envolvendo uma ou mais partes de um processo. Já para os cidadãos, os cartórios em geral representam uma senha para uma nova fila, uma taxa que subiu de novo, uma cópia autenticada da identidade que não ficou boa, ou, no caso dos mais afortunados, finalmente a escritura lavrada de uma casa própria.

A certificação digital, no modelo regulamentado pela ICP-Brasil (Infra-Estrutura de Chaves Públicas) na Medida Provisória 2200-2 de 8/2001, criou uma estrutura hierárquica de autoridades certificadoras, centralizadas em uma autoridade certificadora raiz

e regulada por uma nova agência, o Comitê Gestor da ICP-Brasil. As autoridades certificadoras, bem como as autoridades de registro abaixo delas, formarão um mercado que será regulado por esta agência, sendo cada ente auditado, credenciado e fiscalizado por uma entidade de direito público, o Instituto Nacional de Tecnologias de Informação (ITI), a autoridade certificadora raiz. Hoje ainda testemunhamos os

primeiros passos no sentido da implementação desse sistema, já que são em torno de seis autoridades certificadoras, sendo a maioria órgãos vinculados à União.

Para a economia, a certificação digital representa uma potencial diminuição dos custos de transação que resultam das prerrogativas de certificação dos cartórios. Amplia-se um mercado de certificação de documentos, mais moderno tecnologicamente e mais ágil do ponto de vista do tempo de transação, que certamente fará com que pessoas jurídicas, com cada vez mais frequência, incorram nos custos iniciais de investimento em uma estrutura de certificação digital (seja um *token*, um *smart card* ou uma chave no PC) para poder agilizar e diminuir os custos dessas transações. Em transações internacionais, em particular, ter acesso à certificação digital já está se tornando um imperativo.

Quanto à segurança das transações econômicas, ela será indubitavelmente maior. Uma criptografia assimétrica não é mais manipulável e/ou perigosa do que um carimbo, um selo ou uma rubrica de escrivão de cartório. Há certos mitos sobre as novas tecnologias de informação e comunicação que precisam ser abertamente combatidos e este é um deles.



Computadores são uma das formas mais seguras de armazenamento de informação já concebidas pela humanidade.

Já para o Direito, a certificação digital pode possibilitar uma verdadeira revolução no sistema processual. Com o grau de segurança e sigilo que a internet hoje permite, a certificação digital pode contribuir de forma decisiva para que os tribunais brasileiros esvaziem suas estantes e arquivos de processos. Desde acórdãos com assinatura digital publicados on-line, até a tramitação interna mais cotidiana de processos e seus documentos, a assinatura digital pode ser um instrumento vital que faltava ao Direito brasileiro para que ele, finalmente, converta sua rica estrutura de processamento de litígios e de garantia de direitos em uma ágil rede de interações capaz de mobilizar a capilaridade social de nossos tribunais em práticas democráticas de acesso à justiça para os menos favorecidos.

O sistema processual brasileiro certamente tem suas deficiências institucionais. Entretanto, a sua falta de celeridade resulta primordialmente de um aparato burocrático pouco preparado para acomodar as demandas advindas da sociedade, bem como a energia investigativa de um Ministério Público ativo e independente. Ainda que a informatização não tenha atingido a vasta malha de tribunais de justiça no Brasil, qualquer medida que leve o Estado a fazer os investimentos necessários para tornar o judiciário mais ágil deve ser louvada. Particularmente, se ela aumenta, simultaneamente, o grau de transparência das suas atividades.

Para os cidadãos, no curto prazo, tudo que diz respeito à certificação digital não passa de conversa de gente que mexe com computador. No longo prazo, porém, a inclusão digital é um problema educacional estrutural da sociedade brasileira que precisa ser atacado com políticas públicas dirigidas, porém universais, para que as novas gerações de brasileiros estejam devidamente equipadas com os instrumentos necessários ao pleno exercício da cidadania. A certificação digital é somente mais um prenúncio da premência desta outra agenda já que, caso ela se

consolide e encontre tanto no mercado quanto no poder público a receptividade e atenção que merece, não demorará muito para que nós passemos a ser uma sociedade dividida entre os com-CPF e os sem-CPF, mas também entre os que têm ou não assinatura digital. Seria ela o Registro Geral (R.G.) do futuro?

A grande virtude da Certificação Digital reside na possibilidade da descartorialização do nosso sistema de autenticação e certificação de transações entre entidades de direito civil, sejam elas pessoas físicas ou pessoas jurídicas. Abrir um mercado sem cartórios não é uma garantia contra a sua oligopolização (nem uma idéia tão inovadora assim nos tempos de hoje), mas faz sentido. Faz mais sentido ainda a centralização mantida na estrutura de autoridades constante na medida provisória aprovada sobre o assunto. Haverá sempre um problema de regulação desse mercado, e os agentes públicos e da sociedade civil precisam efetivamente operar nos diversos níveis da burocracia regulatória para agir como efetivos fiscalizadores da qualidade dos serviços de certificação digital oferecidos.

A segurança do sistema virá. Mas pairam dúvidas. Curiosamente, no dia 1º de novembro, a página do ITI para divulgação de seu 2º Fórum de Certificação Digital estava fora do ar, tendo sido invadida por um protesto que clamava "*Nós somos os fora-da-lei de uma lei que não existe*".

Todos, pelo jeito, até mesmo os invasores da página do ITI, aguardam a aprovação do Projeto de Lei 7316/2002, que disciplinará o uso de assinaturas eletrônicas e o mercado de certificação digital. Eu, de minha, parte, espero que, no longo prazo, possamos olhar para os passos que damos hoje como o começo do fim de uma era dos cartórios no Brasil.

**José Eisenberg** - Professor de Ciência Política (IUPERJ), é co-organizador de *Internet e Política: teoria e prática da democracia eletrônica* (Belo Horizonte: Ed. UFMG, 2001) e autor de vários artigos sobre novas tecnologias de informação e comunicação.

# Fonte

A Tecnologia da  
Informação na  
Gestão Pública

Dezembro de 2004

**Contribuições acadêmicas  
exclusivas, focadas nos  
temas certificação digital e  
segurança da informação**



UNIVERSIDADE  

---

CORPORATIVA  

---

P R O D E M G E



# Considerações sobre a interoperabilidade aplicada à infra-estrutura de chaves públicas



## Fabiano Menke

Advogado. Ex-procurador-geral do Instituto Nacional de Tecnologia da Informação. Membro da Comissão Técnica Executiva da Infra-Estrutura de Chaves Públicas Brasileira. Mestre em Direito pelo Curso de Pós-Graduação de Concentração em Direitos Especiais. Professor de Direito Civil no Centro Universitário Ritter dos Reis, Canoas, RS.

## RESUMO

O artigo analisa a interoperabilidade aplicada à Infra-Estrutura de Chaves Públicas (ICP). Principia delineando noção geral de interoperabilidade e, após, versa especificamente sobre a interoperabilidade existente numa ICP. Explica o significado da palavra “infra-Estrutura”, que é de fundamental importância para a análise do objeto de estudo. A abordagem é feita com ênfase na Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), instituída pela Medida Provisória nº 2.200. Além disso, apresenta a interoperabilidade como gênero que se divide em dois, a interoperabilidade formal, operacional, técnica ou objetiva, e a interoperabilidade substancial ou subjetiva.

*Palavras-chave:* interoperabilidade; infra-estrutura (de chaves públicas).

### 1. Noção geral de interoperabilidade

Uma noção geral de interoperabilidade pode ser obtida a partir de um exemplo prático, como o regulado pela Diretiva da Comunidade Européia nº 96/48, de 23 de julho de 1996, que trata da “interoperabilidade do sistema ferroviário transeuropeu de alta velocidade”. Nos considerandos dessa Diretiva, é dito: “para que os cidadãos da União, os operadores econômicos e as

coletividades regionais e locais se beneficiem plenamente das vantagens decorrentes da criação de um espaço sem fronteiras, importa, designadamente, incentivar a interconexão e a interoperabilidade das redes nacionais de trens de alta velocidade, bem como o acesso a essas redes”. Observe-se bem, a Comunidade Européia resolveu adotar uma diretiva estabelecendo critérios e padrões comuns para possibilitar que um trem francês possa sair de Paris, passar por cidades alemãs

e finalmente chegar a Viena, na Áustria, sem que no percurso encontre qualquer problema de incompatibilidade. Para atingir esse objetivo, foram criadas as ETI, que são as especificações técnicas de interoperabilidade, “a que cada subsistema é objeto a fim de satisfazer os requisitos essenciais, estabelecendo as necessárias relações funcionais recíprocas entre os subsistemas do sistema ferroviário transeuropeu de alta velocidade”.

Talvez esse exemplo seja o mais elucidativo para ilustrar o que seja, numa acepção mais geral, interoperabilidade. Por meio dele, verifica-se que a interoperabilidade é um apanágio necessário de qualquer infra-estrutura e pode ser definida como a capacidade que possuem os aparelhos ou equipamentos que dela fazem parte de comunicarem-se entre si, independentemente de sua procedência ou do seu fabricante. Num sistema de telefonia celular, por exemplo, a interoperabilidade permite que dois indivíduos que tenham aparelhos diversos e linhas telefônicas de operadoras diversas possam conversar sem problemas. O mesmo princípio se aplica a uma infra-estrutura de chaves públicas, ou seja, “A” poderá se comunicar eletronicamente com “B”, ainda que os seus certificados digitais e os equipamentos que utilizem para criar e verificar assinaturas digitais não



sejam fornecidos pelo mesmo fornecedor (aqui incluídos a respectiva autoridade certificadora emissora do certificado digital e os fornecedores de *hardware* e *software* utilizados para criar e verificar assinaturas).

## 2. Infra-Estrutura e ICP-Brasil

Não raro, os debates sobre os temas atinentes às assinaturas e certificados digitais fecham os olhos para uma característica fundamental de uma infra-estrutura de chaves públicas (ICP), qual seja, a de que, antes de tudo, e por mais pleonástico e óbvio que possa soar, uma ICP é uma infra-estrutura<sup>1</sup>. E por ser uma infra-estrutura é que a interoperabilidade lhe é ínsita. Portanto, seja qual for a infra-estrutura (de energia elétrica, de saneamento básico, de ferrovias, de telefonia fixa, de telefonia móvel, de chaves públicas, etc.), a palavra interoperabilidade, no mais das vezes, estará presente e dela será um atributo indispensável, sempre que o serviço fornecido tiver por escopo atingir a coletividade.

Insistindo no ponto, uma infra-estrutura de chaves públicas tem o mesmo princípio de qualquer outra instalação estrutural posta à disposição da sociedade, qual seja o de prover um serviço que pode ser obtido por qualquer interessado. Como é sabido, o termo infra-estrutura de chaves públicas é tradução da expressão da língua inglesa: *public-key infrastructure (PKI)*. Os norte-americanos bem souberam esclarecê-la, partindo, primeiramente, da própria definição da palavra infra-estrutura. **Carlisle Adams** e **Steve Lloyd**, na obra *Understanding Public-Key Infrastructure*<sup>2</sup> enfatizaram que uma infra-estrutura se caracteriza por

ser uma *pervasive substrate*, ou seja, uma fundação que dissemine algo para um amplo ambiente ou para um grande universo de interessados. Salientam que duas infra-estruturas comuns são a de comunicações eletrônicas e a de energia elétrica. Asseveram que o princípio de ambas é idêntico: a infra-estrutura existe para que qualquer usuário possa simplesmente acoplar-se a ela e dela fazer uso quando necessário.

A infra-estrutura uniforme evita que sejam aplicadas soluções díspares por cada entidade.

Quanto a esse ponto, é elucidativa a explicação de **Adams** e **Lloyd**: *"The pervasive security infrastructure is fundamentally the sensible architecture for many environments. This architecture avoids piecemeal, point-to-point, ad hoc, non-interoperable solutions, thereby introducing the possibility of manageable, consistent security across multiple applications and computing platforms. It is not difficult to imagine the chaos that would result from every pair of communicants running their own communications lines, or from every person running his/her own power generator at his/her own arbitrarily chosen voltage and current. Many facets of both ancient and modern society demonstrate that the uniformity and convenience offered by a well-designed, well-defined, pervasive infrastructure is worth the effort involved in the design and definition stages"*<sup>3</sup>.

Atente-se bem à observação contida no texto citado: uma infra-estrutura de segurança disseminada, uniforme, evita soluções díspares, isoladas, não interoperáveis. O exemplo fornecido do

caos que resultaria do fato de cada indivíduo operar as suas próprias linhas de comunicação ou de geração de energia é emblemático.

Daí, no meu entender, o acerto da posição adotada pelo Brasil no que toca ao modelo de infra-estrutura de chaves públicas escolhido por meio da Medida Provisória nº 2.200 e regulações posteriores. Sem proibir que o mercado (aqui entendido como o conjunto dos agentes não estatais) implante soluções<sup>4</sup> que podem vir a ser díspares no sentido de não direcionadas à coletividade, decidiu-se por fundar uma espinha dorsal normativa comum, um tronco ou, mais precisamente, uma árvore invertida (*inverted tree*)<sup>5</sup>, situando no topo (na raiz da árvore invertida) uma entidade de direito público, a autarquia federal Instituto Nacional de Tecnologia da Informação – ITI, com as atribuições principais de auditar, credenciar e fiscalizar as autoridades certificadoras, autoridades de registro e prestadores de serviços de suporte que integram a ICP-Brasil.

O modelo adotado pelo Brasil é idêntico ao alemão<sup>6</sup>. Lá, uma divisão do órgão regulador *Regulierungsbehörde für Telekommunikation und Post (Reg-TP)*, com natureza de direito público e vinculada ao Ministério da Economia e Tecnologia, desempenha o mesmo papel que o Instituto Nacional de Tecnologia da Informação, ou seja, credencia, fiscaliza e emite certificados digitais para os prestadores de serviços de certificação (*Zertifizierungsdiensteanbieter*) do primeiro nível hierárquico da cadeia. Até o presente momento, vinte e três *Zertifizierungsdiensteanbieter* já obtiveram credenciamento pe-

rante a RegTP. Entre os credenciados, encontram-se os correios (Deutsche Post), diversas empresas, as entidades de classe dos advogados, as representações de consultores fiscais<sup>7</sup>.

Curiosamente, há que se ressaltar que nos Estados Unidos da América o desenvolvimento e a expansão das infra-estruturas de chaves públicas se deu de forma bastante desorganizada, de sorte que hoje em dia são diversas as ICPs em funcionamento naquele país, com base tanto em iniciativas governamentais quanto em iniciativas privadas.

As razões desse fenômeno são diversas, sendo que um dos motivos principais é o fato de que a autonomia dos estados federados fez com que cada unidade da federação editasse a sua própria lei sobre assinaturas digitais e matérias afins, sem que houvesse uma harmonia principiológica permeando esses diplomas.

Todavia, cientes de que *"PKI is no good if you are only talking to yourself"*<sup>8</sup>, os norte-americanos há alguns anos promoveram a iniciativa do projeto *Federal Bridge Certification Authority*, que tem por escopo fundamental viabilizar a intercomunicação entre os titulares de pares de chaves cujos respectivos certificados sejam provenientes de autoridades certificadoras diversas. Em que pese os esforços, os próprios envolvidos no projeto têm reconhecido que a iniciativa se transformou numa "empreitada que tem sido marcada pelo lento progresso"<sup>9</sup>.

Daí a razão de ser mais racional e de resultados certamente melhores à implementação, desde o princípio, de uma ICP nacional.

Outro aspecto é que, havendo uma ICP mais abrangente, como são a brasileira e a alemã, torna-se bem mais viável e atraente a celebração de acordos internacionais de reconhecimento recíproco de certificados digitais, o que possibilitará transações eletrônicas internacionais mais seguras, entre empresas e entre consumidores e empresas<sup>10</sup>.

No Brasil, as normas a serem cumpridas e observadas pelo ITI e por todas as entidades integrantes da ICP-Brasil são deliberadas pelo Comitê Gestor, que tem na Comissão Técnica Executiva (COTEC) o seu braço técnico e órgão consultivo que examina todas as proposições a serem apreciadas<sup>11</sup>.

Dos estudos da COTEC, e das contribuições advindas da consulta pública realizada em 2001, é que se originaram os documentos básicos da ICP-Brasil, posteriormente aprovados pelo Comitê Gestor. Até o momento, já foram deliberadas cerca de trinta resoluções, mas aquelas que poderiam ser consideradas o núcleo duro normativo são as Resoluções de nºs 1, 2, 7 e 8 (respectivamente, Declaração de Práticas de Certificação da AC Raiz, Política de Segurança da ICP-Brasil, Requisitos mínimos para as Políticas de Certificados e Requisitos mínimos para as Declarações de Práticas de Certificação).

3. Interoperabilidade e ICP-Brasil: interoperabilidade objetiva e interoperabilidade subjetiva

Este conjunto de resoluções e a Medida Provisória nº 2.200-2 contém a base técnica e jurídica da infra-estrutura, e tem como um dos escopos principais garan-

tir a interoperabilidade na utilização dos serviços relacionados à certificação digital, a partir do estabelecimento de padrões<sup>12</sup>. E a idéia que influenciou a criação da ICP-Brasil foi justamente a de constituir uma infra-estrutura para a coletividade<sup>13</sup>, para toda a sociedade, tornando mais facilitada a comunicação entre os titulares de certificados digitais. Evidente que nem tudo está feito, pelo contrário, a implementação das assinaturas digitais certamente trará dificuldades e problemas e mostrará que há muito por fazer para que efetivamente se atinja a desejada interoperabilidade, que deve ser encarada como um desafio, algo em constante construção, e não como algo pronto e acabado, que tenha se esgotado com a simples edição do conjunto normativo mencionado.

E um desses desafios é o relativo à compatibilidade dos cartões inteligentes, leitoras e softwares. Esse ponto é fundamental. Há que se padronizar esses instrumentos, a fim de que, na prática, se tenha a possibilidade de assinar digitalmente, bem como verificar as assinaturas digitais a partir de qualquer equipamento. Por isso, há que se louvar a iniciativa do Instituto Nacional de Tecnologia da Informação em constituir, por meio da Portaria nº 33, de 8 de abril de 2003, grupo de trabalho "para o estudo de padrões com especificações mínimas para o uso de hardwares e softwares na Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil", que redigirá "minuta de resolução que será submetida ao Comitê Gestor da ICP-Brasil" e que tem como uma das finalidades "colaborar na interoperabilidade desses dispositivos"<sup>14</sup>. Realmente, este é um ponto essencial, mas não é só a partir dele

que se explica a interoperabilidade, que, a meu juízo, não termina aí. O que se verifica é que, além dessa interoperabilidade, que eu proporia a denominação de interoperabilidade operacional, formal, técnica ou objetiva, existe uma outra interoperabilidade, que se poderia cunhar de interoperabilidade substancial ou subjetiva. Enquanto que a primeira tem em mira a operação em si, ou seja, a própria criação da assinatura digital e a sua posterior verificação pelo destinatário do documento eletrônico, a segunda, a interoperabilidade subjetiva, vai um pouco além, ela invoca um fundo comum principiológico de índole normativa que faz com que os indivíduos envolvidos na comunicação ou transação eletrônica, seja como signatário, seja como *relying party*, confiem na utilização do serviço, sentindo-se seguros não só aqui e agora, ou seja, no momento da utilização do certificado digital, mas para trás e para frente, isto é, antes e depois de efetuada a transação eletrônica. A preocupação ora enfocada se dirige a aspectos outros, como os relativos aos critérios observados para identificar os titulares de certificados, à forma de geração do par de chaves criptográficas, direitos e obrigações das partes (deveres de indenizar, de contratação de seguro, etc.) e muitos outros que sustentam e regulam a operação técnica da utilização da assinatura digital.

O que se quer dizer com isso é que não basta que os dispositivos de criação e de verificação das assinaturas funcionem aqui e agora. Da mesma forma, não basta que todos os indivíduos envolvidos na transação ou na comunicação utilizem o padrão do formato do certificado X.509. Pre-

tender que a interoperabilidade se resolva apenas a partir da utilização disseminada do padrão X.509 é, sem dúvida, analisar o problema de forma bastante superficial e com total desconhecimento da magnitude envolvida nessa questão.

Por isso, dentre outras coisas, é importante que se tenha confiança de que aquele indivíduo que assinou digitalmente foi corretamente identificado pela autoridade de registro. Assim, Pedro deverá ser realmente Pedro, e não João. Aqui, portanto, vai um primeiro princípio, de suma importância, que é o da identificação do indivíduo mediante a sua presença física<sup>15</sup>, no sentido de tentar evitar, o máximo possível, as fraudes.

Outra norma importantíssima é a da geração do par de chaves pelo próprio titular do certificado, que tem por evidente finalidade evitar a alegação de rejeição da autoria de determinado documento eletrônico pelo titular do certificado, alcançando-se, assim, o denominado não-repúdio<sup>16</sup>. Poder-se-ia citar também as normas referentes ao tempo limite para revogação dos certificados e a frequência de emissão da Lista de Certificados Revogados (LCR)<sup>17</sup>.

Por outro lado, para que a interoperabilidade efetivamente se realize, é preciso que as aplicações que requeiram a utilização da certificação digital não restrinjam o acesso a certificado digital específico, isto é, emitido por apenas uma das autoridades certificadoras. Isso, evidentemente, para os casos de “aplicações voltadas para atendimento ao público em geral, assim considerados, dentre outros, os consumidores,

os contribuintes, os cidadãos, os beneficiários do sistema de saúde, do FGTS, da seguridade social (...)”<sup>18</sup>. Essa norma tem forte conotação de proteção do consumidor, para evitar, na medida do possível e da razoabilidade, que para cada aplicação se tenha que utilizar um certificado digital diferente.

Sem a pretensão de fazer um elenco exaustivo de todas essas regras que constituem esse fundo principiológico normativo comum, chama-se a atenção para um outro ponto, pouco falado, mas de fundamental importância, que é o contido no item 6.3.1 da Resolução nº 7 da ICP-Brasil, que se refere à obrigação das autoridades certificadoras de armazenar, pelo prazo mínimo de 30 anos, as chaves públicas dos titulares de certificados digitais já expirados. Esse é um item essencial. Por meio da observância dele, é possível que se verifique a assinatura digital muito tempo depois de ter sido assinado o documento eletrônico, o que é de suma importância naqueles casos em que se fará necessária a sua posterior apresentação e conferência. Esse prazo é mínimo, por vezes pode haver a necessidade de que as chaves públicas sejam armazenadas por tempo ainda maior<sup>19</sup>. O lapso temporal de 30 anos é devido ao prazo máximo prescricional que poderia haver na legislação. Vale lembrar que, na Alemanha, o certificado de uma autoridade certificadora credenciada é considerado imprescindível, entre outros tantos aspectos, porque há esta obrigação de armazenamento das chaves públicas, que também é de 30 anos a contar do primeiro dia do ano seguinte ao da expiração do certificado digital<sup>20</sup>. Para as entidades que não são creden-

ciadas, a obrigação é de, no mínimo, 5 anos<sup>21</sup>.

Conforme referido, existe, na ICP-Brasil, um sem-número de outros aspectos, tão ou mais importantes do que os alinhados, como a obrigatoriedade de contratação de seguro pelas autoridades certificadoras, segurança dos dispositivos de armazenamento da chave privada, segurança do ambiente físico das autoridades certificadoras, vedação do denominado *key-escrow*, procedimentos de auditoria e de fiscalização, que acabam por constituir esse fundo principiológico comum, de índole normativa, e que geram, ou devem gerar, nos indivíduos integrantes da estrutura e naqueles que utilizam ou conferem os certificados digitais, um sentimento de segurança, e, mais do que isso, a *confiança*, que talvez seja a palavra-chave de uma infra-estrutura de chaves públicas e que os alemães bem souberam utilizar ao qualificarem a sua, denominando-a de *Kette des Vertrauens* (cadeia, ou rede da confiança).

É verdade que nem todos os indivíduos, ao utilizarem o seu certificado digital, estarão conscientes de todos esses aspectos, e também é verdade que fraudes e erros ocorrerão, pois nenhum sistema é de todo imune à falhas, mas o importante é que os usuários tenham um mínimo de segurança e de discernimento de que o máximo foi feito para se evitar problemas, e que se, porventura, algum venha a ocorrer, alguém será responsabilizado, como na hipótese de uma autoridade certificadora encerrar definitivamente as suas atividades, caso em que outra entidade deverá assumir as suas funções, pelo menos no que toca aos certificados digitais já emitidos<sup>22</sup>. Oportuno des-

taçar aqui, também, a importância de o Estado regular e fiscalizar esse incipiente, mas promissor, mercado, haja vista que os consumidores ainda não têm um mínimo de consciência acerca do que significa e do que não significa qualidade no que toca à prestação dos serviços de certificação digital. Quanto a esse aspecto, recomendo expressamente a leitura da resposta número um das FAQs, contida na página da *Regulierungsbehörde für Telekommunikation und Post*<sup>23</sup>, onde é feito um paralelo entre as exigências dos consumidores, motoristas de automóveis, de vinte e cinco anos atrás, e as de hoje.

Assim, verifica-se que para haver interoperabilidade não basta que o simples procedimento da assinatura digital do momento, do aqui e do agora, funcione. É necessário que todo o sistema tenha funcionado satisfatoriamente desde a primeira identificação do primeiro titular de certificado e que continue a funcionar, indefinidamente, de forma razoável. Além disso, será muito difícil que se estabeleçam transações ou comunicações virtuais que demandem segurança se as pessoas naturais ou jurídicas não estiverem regidas e protegidas por um fundo principiológico comum que, além de lhes impor deveres, lhes transmita confiança na utilização do meio eletrônico. Em suma, é importante que os documentos básicos das autoridades certificadoras (as PC e DPC) contenham um mínimo de similaridade quanto aos aspectos primordiais dos serviços, a fim de que seja possível a “conversação”. Daí a importância dessa “outra perna” da interoperabilidade, que enfeixa todos os aspectos citados, que poderia ser chamada, para efeitos ilustrativos, de interopera-

bilidade substancial ou subjetiva.

#### 4. Conclusões

(a) a interoperabilidade é um atributo necessário de qualquer infra-estrutura que pretenda atingir a coletividade, e consiste, numa acepção geral, na capacidade que têm os aparelhos ou equipamentos que fazem parte dessa infra-estrutura de comunicarem-se entre si, independentemente de sua procedência ou do seu fabricante; assim como uma infra-estrutura ferroviária necessita de padrões, uma infra-estrutura de chaves públicas também deverá estabelecer *standards* mínimos a serem observados pelos seus integrantes;

(b) neste sentido, o modelo da ICP-Brasil, previsto na Medida Provisória nº 2.200-2, e que é idêntico ao adotado pela Alemanha e outros países, deve ser considerado razoável, uma vez que, com o estabelecimento de uma espinha dorsal normativa comum, resta bastante facilitada a interoperabilidade;

(c) a noção de interoperabilidade aplicada a uma infra-estrutura de chaves públicas não se esgota no simples funcionamento da criação da assinatura digital, numa ponta, e de sua verificação na outra; portanto, ao lado dessa interoperabilidade objetiva, formal ou operacional, há que se referir à interoperabilidade subjetiva ou substancial, que invoca um fundo principiológico comum, expressado nas normas e padrões, que conferem as necessárias confiança e segurança aos usuários dos serviços de certificação digital;

(d) enfim, a interoperabilidade é algo a ser permanentemente



construído, um desafio constante, que exige esforço de todos os envolvidos. Há, como se sabe, muito a ser feito na ICP-Brasil. Por fim, eu chamaria a atenção para um último ponto que exigirá regulação num futuro bem próxi-

mo e que, salvo meu desconhecimento, pouco tem sido abordado no Brasil com vistas a sua inserção na ICP-Brasil, que é o atinente à necessidade de se proceder a reassinatura (aposição de nova assinatura digital) nos do-

cumentos eletrônicos que necessitam arquivamento por longo período de tempo, tendo em vista que “os procedimentos de criptografia podem perder, ao longo dos anos, seus atributos de segurança”<sup>24</sup>.

---

## Notas

<sup>1</sup> A definição do vocábulo “infra-estrutura” do Dicionário Aurélio, no que toca à área de urbanismo, é a mais adequada à acepção ora enfocada, *in verbis*: “Numa cidade, o conjunto das instalações necessárias às atividades humanas, como rede de esgotos e de abastecimento de água, energia elétrica, coleta de águas pluviais, rede telefônica e gás canalizado.” Vide *Novo Aurélio Século XXI: o dicionário da língua portuguesa*, Aurélio Buarque de Holanda Ferreira. Rio de Janeiro: Nova Fronteira, 1999.

<sup>2</sup> Obra cujo subtítulo é *Concepts, Standards, and Deployment Considerations*. Indianapolis: New Riders, 1999. p. 27.

<sup>3</sup> Ob.cit. p.27-28.

<sup>4</sup> É o que se depreende do parágrafo segundo da Medida Provisória nº 2.200-2, de 24 de agosto de 2001: “O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação de autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados digitais não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento”.

<sup>5</sup> A comparação com a árvore invertida está na obra citada, página 134.

<sup>6</sup> Pelo que se tem notícia, além de Brasil e Alemanha ([www.regtp.de](http://www.regtp.de)), Coreia do Sul ([www.rootca.or.kr](http://www.rootca.or.kr)), Índia ([www.cca.gov.in](http://www.cca.gov.in)), Áustria ([www.rtr.at](http://www.rtr.at)), México e Japão apresentam o mesmo modelo hierárquico com uma entidade de direito público desempenhando o papel de Autoridade Certificadora Raiz. Quanto ao Japão e sua forte inspiração alemã, vide “*Japanische Signaturgesetzgebung – Auf dem Weg zu „e-Japan*”. Artigo de autoria de Alexander Roanagel e T. Yonemaru, Revista Multimedia und Recht, nº 5, volume 12, p. 798 – 806.

<sup>7</sup> Conferir em [www.regtp.de](http://www.regtp.de)

<sup>8</sup> São as exatas palavras proferidas por Peter Alterman, diretor de operações do escritório de pesquisa extra-mural do Instituto Nacional de Saúde dos Estados Unidos da América. Declaração contida no artigo PKI at the crossroads, de autoria de Jennifer Jones, capturado, em <http://www.fcw.com/fcw/articles/2002/0624/tec-pki-06-24-02.asp>, no dia 04.07.2002.

<sup>9</sup> Idem anterior. O texto original diz o seguinte: “*Years in the works, a federal effort to link the public-key infrastructures (PKIs) of agencies has proved quite an undertaking and has been marked by that appears to be rather slow progress*”.

<sup>10</sup> O art. 4º, inciso VII, da MP 2.200-2, determina que compete ao Comitê Gestor da ICP-Brasil “identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais”.

<sup>11</sup> Sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira e a Comissão Técnica Executiva, vide o Decreto nº 3.872, de 18.07.2001. Sobre a necessidade de a COTEC manifestar-se previamente sobre todas as matérias a serem apreciadas pelo Comitê Gestor, vide art. 4º, parágrafo terceiro, inciso I do aludido decreto.

<sup>12</sup> De maneira que foi absorvida e ampliada, pela ICP-Brasil, a iniciativa da ICP-Gov de que tratava o revogado Decreto nº 3.587, de 5.09.2000.

<sup>13</sup> Vide os considerandos da Portaria nº 33, de 08.04.2003.

<sup>14</sup> Esta exigência foi determinada no art. 7º da Medida Provisória nº 2.200-2 e reafirmada no item 3.1.9 da Resolução nº 7.

<sup>15</sup> Vide o parágrafo único do art. 6º da MP 2.200-2 e item 6.1.1 da Resolução nº 7. O não-repúdio é uma presunção relativa de que aquele que assinou digitalmente, a princípio, estará vinculado à declaração de vontade manifestada. Por ser uma presunção relativa ou *juris tantum*, é possível a prova em contrário. Por exemplo, o suposto autor da manifestação de vontade poderá provar que foi coagido a assinar determinado documento eletrônico, e, assim, fazer cessar a presunção de autoria. Todavia, tudo dependerá da análise do conjunto probatório, e se o caso chegar ao Poder Judiciário, o magistrado competente deverá investigar fatos como, se após cessada a coação, o coagido tomou as devidas cautelas para comunicar ao destinatário da mensagem sobre o ocorrido, a fim de paralisar eventual execução contratual (comunicando até mesmo a necessidade de revogação do certificado perante a autoridade certificadora). Enfim, existem infinitas possibilidades de combinação de fatos que deverão ser analisados com prudência e cuidado pelo juiz.

<sup>16</sup> Estes procedimentos estão estabelecidos nos itens 4.4.3 a 4.4.9 (vide também anexo I), da Resolução nº 7.

<sup>17</sup> Como dispõe o item 1.3.4 da Resolução nº 7, que assim continua “(...), que aceitarem certificados de um determinado tipo previsto pela ICP-Brasil, devem aceitar todo e qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitidos por qualquer AC integrante da ICP-Brasil”.

<sup>18</sup> Casos de documentos eletrônicos que tenham de ser arquivados por prazos de tempo ainda maior. Por exemplo, caso os registros de imóveis e os arquivos de registros civis venham a armazenar os seus registros de forma eletrônica, o armazenamento das chaves públicas certamente deverá ser por prazo indeterminado.

<sup>19</sup> Quanto a este aspecto, vide o item 2 do parágrafo quarto do Decreto de Assinatura alemão, de 16.11.2002, o denominado *Signaturverordnung*. Na doutrina alemã, quanto a este aspecto e quanto à valorização e à indispensabilidade do certificado digital fornecido por autoridade certificadora credenciada perante a *Regulierungsbehörde für Telekommunikation und Post*, vide Alexander Roanagel, no artigo **Rechtliche Unterschiede von Signaturverfahren**, publicado na Revista Multimedia und Recht, nº 4, 2002, p. 215-222.

<sup>20</sup> Vide o item 1 do parágrafo quarto da *Signaturverordnung*.

<sup>21</sup> Daí ser de extrema importância o disposto no parágrafo 3º do art. 11 do Projeto de Lei nº 7.316/2002, uma vez que dispõe que, em último caso, a própria AC Raiz, como a âncora de confiança do sistema, acaba por assumir os documentos relativos aos certificados já emitidos por entidade que venha a encerrar as suas atividades.

<sup>22</sup> [www.regtp.de](http://www.regtp.de)

<sup>23</sup> Tradução livre que fiz de trecho do excelente artigo de Ralf Brandner, Ulrich Pordesch, Alexander Roanagel e Joachim Schachermayer, sob o título **Langzeitsicherung Qualifizierter Elektronischer Signaturen** (A proteção duradoura das assinaturas eletrônicas qualificadas), que versa especificamente sobre o tema, publicado na Revista DuD – Datenschutz und Datensicherheit, nº 2/2002, p. 97-103.



# A privacidade na ICP-Brasil



## Alexandre Rodrigues Atheniense

Advogado. Sócio da Aristóteles Atheniense Advogados S/C. Coordenador do Curso de atualização de Direito na Informática na PUC Minas Virtual. Presidente da Comissão de Informática do Conselho Federal da Ordem dos Advogados do Brasil. Presidente da Comissão de Informática da Seccional de Minas Gerais da Ordem dos Advogados do Brasil. Vice-presidente jurídico da Sucesu-MG.

## RESUMO

O artigo apresenta a delimitação do conceito de privacidade, assim entendido pela doutrina clássica do Direito. Procede-se, então, a uma análise da tutela constitucional da intimidade e da vida privada. Clarifica-se, para fins meramente didáticos, a distinção existente entre os termos "intimidade" e "vida privada". São traçadas algumas linhas a respeito da ideologia da infra-estrutura de chaves públicas, implementada pela Medida Provisória nº 2.200-2, analisando a doutrina nacional a seu respeito. Parte-se, assim, para as críticas a serem feitas em relação à instituição de um certificado único para os usuários e à possibilidade de se realizar análise de tráfego dos certificados revogados pelas autoridades certificadoras.

*Palavra-chave:* privacidade (na ICP-Brasil).

### 1. O conceito do direito à privacidade

O direito à privacidade tem consistido em objeto de estudo de inúmeros juristas ao longo dos anos. No entanto, revela-se, em certa medida, ingrata, a difícil tarefa a que alguns se propunham de delimitar sua abrangência na vida social.

Cumprido esclarecer, portanto, antes de adentrarmos à análise conceitual desse direito, a própria etimologia da palavra, que deriva do termo latino *privatus*, e que,

segundo SAMPAIO (1998)<sup>1</sup>, significa *fora do Estado, pertencente à pessoa ou ao indivíduo mesmo*.

É assim que podemos conceituar a privacidade como uma faculdade inerente a todo e qualquer indivíduo de manter fora do alcance de terceiros o conhecimento sobre fatos inerentes a sua própria pessoa ou atividades particulares.

É o direito à privacidade, destarte, um direito eminentemente subjetivo, delimitado pela própria

cognição do indivíduo. Nesse sentido, assinalou a melhor doutrina norte-americana ao decidir, no caso *Katz vs. United States*, que o direito à privacidade do indivíduo não se estenderia apenas à sua casa e documentos, mas também a qualquer lugar no qual ele pudesse ter *razoável expectativa de privacidade*.

A privacidade concebida em seu sentido lato ainda pode ser entendida como "o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito" (SILVA, 2001)<sup>2</sup>.

O direito à privacidade é, dessa maneira, excepcional, na medida em que consiste num direito negativo, ou seja, expresso exatamente pela não-exposição a conhecimento de terceiro de elementos particulares da esfera reservada do titular (BITTAR, 2001)<sup>3</sup>. Mera espécie do direito à privacidade é o direito à autodeterminação informativa, criação da doutrina espanhola, e comentado por COSTA (2001)<sup>4</sup>:

"Passados pouco mais de 100 anos daquela publicação, vivemos hoje também a necessidade da criação de um novo direito do cidadão, curiosamente nascido daquele direito à privacidade, que acabou consagrado no último século, fundado nas mesmas razões do desenvolvimento tecnológico e de métodos comerciais,

agora por causa da informática e da telemática, e pautado naquela mesma expressão singela, mas marcante, de que nos deixem em paz, direito esse que se constitui na proteção do cidadão em face do tratamento automatizado de seus dados (...).”

No entanto, decerto que a abrangência desse direito não é incondicional. GODOY (2002)<sup>5</sup>, citando CALDAS, nos lembra que: “(...) a vida privada do indivíduo presente, necessariamente, uma face pública, consubstanciada nas contingências da vida de relações, da vida profissional de alguém, de sua obrigatória exposição, (...) essa exposição será maior, a limitar a privacidade, de acordo com a atividade da pessoa (...)”.

Assim é que podemos concluir que o direito à privacidade será tanto menor quanto maior seja a notoriedade ou publicidade do indivíduo, estando certos de que a liberdade de imprensa também é um direito resguardado pela nossa Constituição.

## 2. A proteção constitucional da intimidade e da vida privada

A Constituição Federal consagrou, em seu artigo 5º, inciso X, que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Não obstante, temos a privacidade como valor constitucional inserto no seletor rol de direitos e garantias fundamentais da pessoa humana, sem os quais não se poderia assegurar uma convivência digna e igualitária do tecido social. Nesse particular, vale a

ressalva do art. 60, §4º da Lei Magna que erigiu tal garantia à condição de cláusula pétrea.

Custosa é a distinção doutrinária ao analisar a disparidade entre os termos intimidade e vida privada, inculpidos no rol de garantias individuais de nossa Carta Magna. A doutrina converge, conforme assinala GODOY (2002)<sup>6</sup>, no sentido de que, quando se procura diferenciar vida privada e intimidade do indivíduo, estabelece-se, entre os conceitos, verdadeira relação de gênero e espécie.

E continua, agora citando SERRANO: “(...) privacidade qualificada, na qual se resguarda a vida individual de intromissões da própria vida privada, reconhecendo-se que não só o poder público ou a sociedade podem interferir na vida individual, mas a própria vida em família, por vezes, pode vir a violar um espaço que o titular deseja manter impenetrável mesmo aos mais próximos, que compartilham consigo a vida cotidiana”.

Em que pesem os argumentos de CASTRO (2002)<sup>7</sup> e SZANIAWSKI (1993)<sup>8</sup>, entendemos ser mera dedução lógica o entendimento de que a intimidade consiste em uma vertente do direito à vida privada, estando ambos previstos no bojo da Norma Constitucional em razão de má-técnica legiferante.

De acordo com o *iter* até aqui traçado, resta claro que a privacidade há de ser assegurada independentemente do meio escolhido para a prática de quaisquer atos jurídicos, inclusive o eletrônico, ora objeto desta análise.

Nesse íterim, não podemos entender a privacidade como o direito de estar só, há anos

conclamado pela doutrina anglo-saxônica, mas, sim, como um direito de manter-se, e à sua propriedade, fora do controle de terceiros, o que englobaria, necessariamente, o liame residual competente a cada indivíduo de impedir o acesso e a divulgação de informações sobre sua vida privada.

## 3. O direito à privacidade e sua tutela jurídica

O desenvolvimento de sistemas informáticos tem feito com que a busca pela tutela jurídica efetiva dos direitos da personalidade seja posta em evidência. Assim, podemos notar uma tendência à disciplina desses direitos em alguns códigos modernos, tais quais o italiano (artigos 5 a 10) e o português (artigos 70 a 81).

BITTAR (2001) assinala que *incursões* na vida privada, especialmente ditadas pela evolução da tecnologia e das comunicações, têm exigido o reconhecimento expresso desses direitos e a sua regulamentação, para garantir-lhes proteção no âmbito privado.

No Código Civil Brasileiro de 2002, deixou, o legislador, de tratar do direito à intimidade de forma precisa, limitando-se a estabelecer, em seu artigo 21, que a vida privada é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

A privacidade dos indivíduos é resguardada, portanto, não só em relação a fatos inerentes à sua vida privada, profissional e familiar, mas, também, em relação às suas informações pessoais. Tal qual é a importância dessa proteção, que o Código de Defesa

do Consumidor tutelou, em seu artigo 13, incisos X a XV, algumas condutas consideradas ilícitas em relação à manipulação de informações dos consumidores, quais sejam: impedir ou dificultar o acesso gratuito do consumidor a informações em cadastros, fichas ou registros de dados pessoais (...); elaborar cadastros de consumo com dados irreais ou imprecisos; deixar de comunicar ao consumidor, no prazo de cinco dias, as correções cadastrais por ele solicitadas; etc.

Não obstante a tutela jurídica das informações no âmbito privado, previu, a Constituição Federal, ação mandamental destinada à ciência de informações contidas em bancos de dados pertencentes a entidades públicas ou de caráter público, o *habeas data*.

Assim sendo, em se tratando de entidade ligada à Administração Pública, compete ao indivíduo um instrumento processual adequado como garantia dos direitos previstos no artigo 5º, inciso X (supracitado), XXXIII (direito a receber dos órgãos públicos informações de seu interesse particular) e XXXIV, “b” (obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimentos de situações de interesse pessoal).

Podemos notar, deste modo, que a tutela jurídica da vida privada, dada sua importância, encontra amplo respaldo seja na Constituição Federal, seja em lei infra-constitucional.

#### 4. A infra-estrutura de chaves públicas

O desenvolvimento econômico da internet certamente gera uma demanda para que os negócios

ali realizados sejam acobertados por um certo nível de segurança jurídica. Assim, surge a necessidade tanto da transmissão quanto do conteúdo das informações que trafegam na rede serem conservadas fidedignas para que possam servir de substrato tanto como prova de uma relação ocorrida quanto do convencimento do magistrado em uma eventual lide.

Dessa maneira, insurge-se falar sobre o papel de um terceiro, estranho à relação jurídica e portanto dotado de neutralidade, que detém poderes bastante para autenticar a identidade dos usuários e certificar a autenticidade tanto do conteúdo quanto da transmissão das informações em uma rede, *a priori*, insegura.

Tal qual é a opinião de BARRETO (2001)<sup>10</sup>:

“O papel dos terceiros certificadores insere-se perfeitamente nessa lógica de proporcionar segurança nas transmissões de dados via internet, sem que haja contudo ingerência no conteúdo de tais transmissões, bem como fornecer provas irrefutáveis que possam ser aceitas pelas partes em caso de litígio”.

Esse foi o espírito que motivou a edição da Medida Provisória 2.200-2, de 24 de agosto de 2001, que, dentre outros, instituiu a Infra-estrutura de Chaves Públicas no País.

De imediato, causa-nos estranheza que uma norma de tamanho impacto social seja elaborada por um ato do executivo, o que não deveria ocorrer em uma democracia representativa.

Em que pesem as críticas, instituiu a referida MP, o arcabouço fundamental concernente à vali-

dade jurídica do documento eletrônico. Através deste ato emanado pelo Poder Executivo, adotou-se uma estrutura centralizada – vertical – para a expedição de certificados eletrônicos.

Essa estrutura vertical, por sua vez, foi constituída sob a premissa de que um único certificado digital emitido para o usuário final se prestaria à prática de todos os atos da vida civil, facilitando, assim, a interoperabilidade entre os sistemas de certificação.

Com toda a *venia* às opiniões contrárias, entendemos que a adoção de um certificado único em nada facilitaria a interoperabilidade do sistema por absoluta inexistência de nexo causal entre os fatos.

A simples exigência da observância do credenciamento perante a AC-Raiz, por si só, representaria um risco social e um ônus insuportável a cargo do indivíduo.

A interoperabilidade entre as autoridades certificadoras é relacionada, sim, com o modelo de certificação adotado no mercado, tal como o X.509. BARRETO<sup>11</sup> traz a lume uma interessante ilustração: “Esse modelo é frequentemente referido como o modelo do cartão de crédito, na medida em que reflete o modelo comercial no qual a indústria do cartão de crédito se baseia. Na indústria do cartão de crédito, o que faz o comerciante aceitar o cartão de crédito apresentado pelo consumidor como forma de pagamento é o fato de o cartão ter sido emitido por um banco que ele conhece ou, ainda que o comerciante nunca tenha ouvido falar do banco que emitiu o cartão de crédito, esse banco terá sido certificado por uma companhia de

cartões de crédito (...).

Do momento em que o comerciante conheça e confie na companhia de cartões de crédito, ele poderá confiar no banco e no consumidor, e assim aceitar aquele cartão de crédito como forma de pagamento”.

E continua a referida autora: “A abordagem hierárquica do padrão X.509 oferece algumas vantagens, ao permitir que inúmeros certificados se relacionem a uma mesma raiz confiável”.

Mas o repúdio à estrutura do certificado único não se dá única e exclusivamente em razão de sua interoperabilidade, mas pela ameaça da instituição de um número único para cada indivíduo.

#### 4.1. A adoção do certificado único

A implementação de um certificado único envolveria a congregação de todas as informações acerca do indivíduo em um mesmo suporte, para se compatibilizar à ampla gama de serviços oferecidos no meio eletrônico. Nesse diapasão, assevera SILVA<sup>12</sup> que “o amplo sistema de informações computadorizadas gera um processo de esquadramento das pessoas, que ficam com sua individualidade inteiramente devassada”<sup>2</sup>.

Cumprir lembrar que, no final de 1995, a Comunidade Européia editou a diretiva 95/46 segundo a qual os “Estados Membros devem proteger os direitos e liberdades fundamentais das pessoas naturais, e em particular seu direito à privacidade em relação ao processamento de dados pessoais”.

Além disso, a própria Constitui-

ção Portuguesa vedou expressamente a adoção de um número único exatamente por antever os efeitos que poderiam ser causados pela prática deste ato, *in verbis*:

**“Art. 35.** Utilização da informática:

5 – É proibida a atribuição de um número nacional único aos cidadãos”.

Com efeito, a instituição de um certificado único, como quer implementar e regulamentar o CG – ICPBrasil, acabaria por comprometer a individualidade, intimidade e privacidade do cidadão. Não se pode elidir tal garantia sob a pretensa alegação de facilidade na utilização. Ademais, a instituição de uma AC Raiz (árvore única) garante o monopólio das informações por parte desta instituição, quando o mais seguro seria pulverizar as informações sobre o indivíduo em vários certificados, permitindo-se várias AC Raiz em um sistema floresta. A existência de uma única raiz é justificada pelo fato de permitir a interoperabilidade entre as ACs, entretanto, essa famigerada interoperabilidade pode ser alcançada através da adoção de padrões tecnológicos comuns (v.g. X.509).

A violação de um banco de dados contendo todas as informações pessoais (que será a tônica em um ambiente com certificado único) de um determinado indivíduo representaria um risco social insuportável na medida que sua vida privada poderia ser completa e indevidamente devassada. A utilização de aparatos informáticos facilita o tratamento da informação. Assim, esta violação não atingiria somente o âmbito de relacionamento do in-

divíduo com o órgão em questão, mas todo relacionamento daquele com a sociedade. Bem assevera GRECO (2000)<sup>13</sup> ao afirmar que: “numa sociedade complexa (...) o poder advém da posse de informações sobre pessoas, eventos ou coisas”<sup>3</sup>.”

A existência destes vários cadastros é, na verdade, uma garantia de que o indivíduo não terá sua vida devassada na medida em que dificulta o cruzamento de tantas informações complexas. Essa é a principal razão pela qual a instituição de um certificado único foi rechaçada pelos países europeus.

#### 4.2. A análise de tráfego

Outra questão controvertida em relação a ICP-Brasil concerne à análise de tráfego da consulta dos certificados revogados. Na utilização de um certificado digital, a verificação da lista de certificados revogados, mantida pela autoridade certificadora, poderia gerar, para diversos fins, um *log*, que em última análise pode fornecer algumas informações sobre aquele usuário.

Apesar de não ser capaz de acessar o conteúdo da mensagem em razão da certificação digital, o simples fato de ter ciência da comunicação seria capaz de ameaçar a privacidade dos usuários, uma vez que muitas informações podem ser obtidas através da análise do perfil (intervalo de tempo, tamanho, datas e horários das mensagens) dessas mensagens. A violação da privacidade do indivíduo poderia dar-se não pelo conhecimento do conteúdo que foi transmitido, mas de uma forma muito mais sutil, através do conhecimento da existência de comunicação



entre as partes. Afirma o professor SCHNEIER<sup>14</sup> que “often the patterns of communication are just as important as the contents of communi-

cation”<sup>4</sup>. Diante dessas considerações, reiteramos a crítica no sentido de não privilegiar o avanço tecnológico em detrimento dos direitos

e garantias fundamentais. E, ainda, compatibilizar a regulamentação da ICP Brasil com a ideologia constitucionalmente adotada.

---

## Notas

<sup>1</sup>. SAMPAIO, José Adércio Leite, *Direito a Intimidade e à Vida Privada*, Belo Horizonte: Del Rey, 1998, p.34

<sup>2</sup>. SILVA, José Afonso da Silva, *Curso de Direito Constitucional Positivo*, 19ª ed., São Paulo: Malheiros, 1997, p.209

<sup>3</sup>. BITTAR, Carlos Alberto, *Os Direitos da Personalidade*, 5ª ed. rev., atual., ampl. por Carlos Bianca Bittar. Rio de Janeiro: Forense, 2001, p. xx, p. xx, p. 108

<sup>4</sup>. COSTA, Marcos da, *Novos Ventos Digitais*, disponível em: [http://www.marcosdacosta.adv.br/documento.asp?ID\\_Documento=455](http://www.marcosdacosta.adv.br/documento.asp?ID_Documento=455) - acesso em: 15/05/2003

<sup>5</sup>. GODOY, Cláudio Luiz Bueno de, *A Liberdade de Imprensa e os Direitos da Personalidade*. São Paulo: Atlas, 2001, p.47;

<sup>6</sup>. Op. Cit. 5, p. 49

<sup>7</sup>. CASTRO, Mônica Neves Aguiar da Silva, Honra, *Imagem, Vida Privada e Intimidade em Colisão com Outros Direitos*. Biblioteca de Teses. Rio de Janeiro: Renovar, 2002, p.32

<sup>8</sup>. SZANIAWSKI, Elimar, *Direitos da Personalidade e sua Tutela*. São Paulo: RT, 1993, p. 132

<sup>9</sup>. Op. Cit. 3, p.35

<sup>10</sup>. BARRETO, Ana Carolina, *Assinaturas Eletrônicas e Certificação*, In: ROCHA FILHO, Valdir de Oliveira (coord.), *O Direito e a Internet*, Rio de Janeiro: Forense Universitária, 2002, p.44

<sup>11</sup>. Op. Cit. 10, p.48

<sup>12</sup>. Op. Cit. 2, p.212

<sup>13</sup>. GRECO, Marco Aurélio, *Internet e Direito*, 2ª ed., rev. e aum., São Paulo: Dialética, 2000, p.194

<sup>14</sup>. SCHNEIER, Bruce, *Secrets & Lies Digital Security in a Networked World*, Wilye Computer Publishing, 2000, p.34

---



# Tudo que você deve saber sobre certificação digital



## Jeroen van de Graaf

Pesquisador em criptografia há mais de 20 anos e doutor na área pela Universidade de Montreal, Canadá. Atualmente, trabalha como pesquisador na UFMG e atua como consultor autônomo através da sua empresa, a VDG-InfoSec.

## RESUMO

No mundo convencional de papel, estamos acostumados às propriedades de autenticidade, integridade e não-repúdio de documentos que, juntas, criam a fé indispensável para quase todos os processos burocráticos. Para um mundo digital (sem papel) dar certo, é necessário que essas propriedades continuem valendo. Este texto tenta explicar as noções básicas das novas tecnologias que estão surgindo para garantir a fé de documentos no mundo digital: a assinatura digital, o certificado digital e a infra-estrutura de chaves públicas, entre outros.

O texto tenta simplificar o máximo possível. No entanto, também não é desejável simplificar demais esse assunto complexo e fascinante; senão há o risco de perder a essência e enganar o leitor. Espero que minha tentativa contribua para a compreensão desse assunto por um público maior.

### 1. Assinar um documento convencional

Todo mundo já assinou um documento. A única observação importante é que cada assinatura é igual (em teoria), e que a ligação entre o texto do documento e a assinatura é o meio físico subjacente: o papel.

### 2. Assinar um documento digital

Uma assinatura digital é o resul-

tado de uma computação que tem duas entradas: um documento eletrônico e uma chave criptográfica e secreta. A computação embaralha todos os bits do documento e da chave, resultando numa seqüência de bits de tamanho fixo (normalmente 1024 bits). Esta é a assinatura digital, que é anexada ao documento original.

Uma assinatura digital tem a seguinte característica: sem acesso à chave secreta, é matematicamente impossível calcular qual a

seqüência de bits que constitui a assinatura digital. Claro, um forjador sempre pode “chutar” uma assinatura. Mas a probabilidade de acertar corresponde a ganhar a MegaSena 40 vezes seguidas, um evento tão improvável que, na prática, pode ser mesmo desconsiderado.

Observe que a autenticidade e o não-repúdio do documento assinado digitalmente se baseiam no conhecimento da chave: quem é dono da chave secreta é autor daquele documento. Portanto, o sigilo da chave é de suma importância. A integridade do documento se baseia numa outra característica do método da computação: se um bit do documento original for mudado, a assinatura sai completamente diferente; então, adulterar um documento assinado é impossível.

A assinatura digital se parece muito com a assinatura de punho, ou com o selo do mundo tradicional de papel. No primeiro exemplo, a chave secreta corresponde aos movimentos motores do assinante e, no segundo, é supostamente impossível recriar (ou seja, forjar) o selo, com sua estrutura fina de linhas, papel e tinta especial, etc. Como no mundo digital não há meio físico, a assinatura depende não apenas da chave, mas também do documento. Obviamente, deve ser assim; senão seria muito fácil cor-

tar uma assinatura digital de um documento e colá-la embaixo de um outro.

### 3. Verificar uma assinatura convencional

Até agora, falamos apenas sobre como assinar documentos, mas igualmente importante é como se verifica uma assinatura. Para entender mais tarde a verificação no mundo digital, é importante lembrar como isso funciona no mundo tradicional. São procedimentos tão cotidianos que é fácil se esquecer da sua importância. Para assinaturas de punho, é comum que um indivíduo se dirija pessoalmente a uma “autoridade” (um banco, um cartório). A autoridade confere a identidade da pessoa e cria uma ficha com dados pessoais e outros dados relevantes, e com a assinatura daquela pessoa. Em princípio, depois dessa visita, o indivíduo nunca mais precisa voltar. Quando um terceiro mostrar à autoridade um documento supostamente assinado por aquele indivíduo, ela procura a ficha, compara as duas imagens das assinaturas e dá um veredicto: a assinatura é válida ou não. Com selos, a situação é um pouco diferente, eles são emitidos por órgãos que já têm autonomia, então, não precisam de uma autoridade. Mas, nesse caso, também devem existir modelos para que terceiros possam comparar.

### 4. Verificar uma assinatura digital

No mundo digital, a verificação de uma assinatura é muito parecida, e em alguns pontos até mais flexível. Dada a chave secreta que é usada para assinar, é possível criar uma outra chave pública correspondente, que é usada na ve-

rificação da assinatura. Esse par de chaves tem uma característica surpreendente: mesmo conhecendo a chave pública, é matematicamente impossível calcular a chave secreta correspondente. Este modelo é conhecido como criptografia com chaves públicas. É diferente da criptografia convencional descrita nos livros de espionagem: neles, a chave para cifrar e decifrar deve ser a mesma, e ela não pode ser pública.

No mundo convencional, a chave secreta (também chamada de chave privada) corresponde aos movimentos motores do indivíduo, enquanto a chave pública corresponde à imagem da assinatura no papel, um dado que é público. E como no mundo convencional é necessário vincular a imagem da assinatura a uma identidade, é necessário que exista o mesmo procedimento no mundo digital. O indivíduo se dirige a uma autoridade com a sua chave pública (e talvez com outros documentos comprovando sua identidade), a autoridade confere a identidade da pessoa e cria uma ficha com os dados pessoais e a chave pública daquela pessoa.

Mas, em vez de guardar essa ficha no seu arquivo, a autoridade assina-a e publica-a na internet! É esse documento, contendo uma chave pública e os dados pessoais do seu dono, que é chamado um certificado digital. Ou seja, o certificado digital corresponde à ficha do cartório, carimbada pelo tabelião, publicada livremente. Um certificado digital não é sigiloso; ao contrário, pode e deve ser copiado e distribuído à vontade. A grande vantagem é que qualquer pessoa, em qualquer lugar no mundo com acesso à internet, pode verificar a assinatura.

Em outras palavras, verificar uma assinatura digital é parecido com verificar uma assinatura convencional: têm-se o documento assinado e o certificado digital; o último contém a identidade do assinante e a sua chave pública. E, através de uma segunda computação matemática, verifica-se se os dois conferem, ou seja, se a chave secreta usada para assinar o documento corresponde à chave pública no certificado.

### 5. Infra-estrutura de Chaves Públicas (ICP)

Note bem como funciona a cadeia de confiança no exemplo anterior: a identidade do assinante é garantida pela autoridade que emitiu (assinou) o certificado digital, comumente chamada Autoridade Certificadora (AC). Ou seja, é necessário que o verificador conheça a chave pública daquela AC para verificar se o certificado foi realmente assinado por ela. É nesse ponto que as coisas se complicam.

Como existem milhares de bancos e cartórios geograficamente espalhados no Brasil e no mundo, é claro que devem existir milhares de ACs. Mas é inviável que um verificador conheça todas as chaves públicas dessas autoridades. Portanto, por motivos de escalabilidade, existem “meta-autoridades”, que credenciam autoridades intermediárias, que emitem certificados a indivíduos.

O resultado é uma hierarquia de autoridades certificadoras: existe apenas uma AC-Raiz cujo único papel é emitir certificados para suas AC-intermediárias. Elas, por sua vez, emitem certificados para os indivíduos ou entidades pertencentes à hierarquia. Um sentido do termo Infra-estrutura de Chaves Públicas (ICP) é essa hierar-



quia (ou árvore) de certificação. Por exemplo, na ICP-Brasil há uma AC-Raiz e seis ACs-Intermediárias de primeiro nível: a Presidência da República, a Serasa, a Receita Federal, o Serpro, a Caixa Econômica Federal e a CertiSign.

Aliás, existe um outro uso da sigla ICP (PKI=Public Key Infrastructure, em inglês), o que cria bastante confusão. Como deve ser óbvio, existe uma quantidade enorme de padrões, software, hardware, procedimentos e documentos para essa tecnologia funcionar. O termo Infra-estrutura de Chaves Públicas (ICP), no sentido amplo, é usado também para se referir a esse conjunto, à tecnologia em geral.

Felizmente, existe um padrão adotado mundialmente (PKIX-X.509) e existe software livre para construir uma ICP (hierarquia). Por exemplo, o meu notebook contém um software para criar uma ICP funcional. No entanto, esse programa só serve para pesquisa, não é uma solução viável para gerenciar uma ICP com centenas de certificados. Mesmo assim, há uma implicação importante aqui: qualquer pessoa pode criar uma ICP. A padaria na esquina, o Minas Tênis Clube, a UFMG, o Estado de Minas Gerais, todo mundo pode emitir certificados. Então, se não houver impedimentos técnicos para emitir certificados, qual é a credibilidade (o valor) de um certificado?

## 6. A credibilidade de certificados

Nesse contexto, uma outra comparação com o mundo tradicional é muito interessante. Nossa carteira é cheia de documentos

que atestam nossas credenciais: carteira de identidade, carteira de motorista, cartões de crédito, carteirinha da biblioteca da UFMG, carteirinha da videolocadora, carteirinha de seguro de saúde, etc., etc. A credibilidade dessas não depende do documento em si, mas da política de quem o emitiu. Por exemplo, a credibilidade de um cartão American Express Platinum é diferente da do cartão Carrefour. E a carteira de identidade tem uma grande credibilidade para terceiros, porque todo mundo sabe que há um processo rigoroso por trás para consegui-la, enquanto a carteirinha da videolocadora não tem validade nenhuma porque todo mundo consegue facilmente.

Com certificados digitais é igual: a sua credibilidade depende completamente da política adotada pela autoridade certificadora emissora. Por exemplo, existe um site na internet que emite certificados automaticamente, sem verificação nenhuma e, portanto, sem credibilidade nenhuma, mas mesmo assim é útil para testes. Existem empresas que emitem um certificado a qualquer cidadão com nome, CPF e título de eleitor, após a verificação desses dados, cobrando uma taxa de 100 reais anual. E para ser AC-intermediária subordinada à AC-Raiz da ICP-Brasil é necessário pagar centenas de milhares de reais como taxa (sem falar dos custos para montar uma sala-cofre, que custa milhões, para guardar a chave privada). Lembre-se que, em todos os casos, estamos falando de certificados que são simplesmente bits, nem possuem um holograma bonito. Repito, a credibilidade do certificado advém da credibilidade da AC. Aliás, introduzindo carteiras de

identidade, mudamos sutilmente de assunto. Em vez de discutir a assinatura digital, que provê autenticidade, integridade e não-repúdio de documentos, estamos discutindo identificação: como estabelecer a identidade de pessoas. E, em muitas situações, ela é importante, porque associada a ela estão privilégios e direitos, por exemplo, o direito de dirigir um carro. Ou seja, a identificação leva a uma autorização. A tecnologia ICP serve também para implementar a identificação e autorização das pessoas no mundo digital.

Ainda por cima, a mesma tecnologia também pode ser aplicada para proteger o sigilo de documentos e comunicações, mas, na maioria das situações, as organizações não se preocupam com o sigilo, e, sim, com a fé dos documentos e processos, ou seja, com as questões de autenticidade, integridade e não-repúdio de documentos, e identificação de pessoas.

## 7. O lado comercial da certificação digital

O valor econômico dessa tecnologia foi logo percebido nos anos oitenta, mas explodiu com a chegada da internet. Em particular, o certificado digital é um mecanismo poderoso para estabelecer uma identidade digital das pessoas. Como explicamos, ele serve para assinar documentos, e também para comprovar a identidade. As maioria das empresas que atua nessa área ganha dinheiro cobrando pela emissão de certificados. As empresas colocam um prazo de validade de um ano, normalmente, garantindo uma fonte de renda regular. Na realidade, muitas vezes elas deixam de explicar a seus clientes

que criar uma própria ICP poderia ser uma opção interessante, dependendo das circunstâncias.

## 8. A ICP-Brasil

A ICP-Brasil foi uma iniciativa do governo anterior com a intenção de unificar a certificação digital no Brasil. Ela passa a impressão de que deve existir uma única ICP no Brasil, com ela ao topo. A própria palavra “infra-estrutura” pode levar o leigo a crer nisto, inconscientemente fazendo a analogia com a rede elétrica num país. Porém, a analogia certa é com a telefonia celular: podem existir vários operadores de telefonia celular paralelamente.

Não é sempre preciso aderir à ICP-Brasil para usar a certificação digital, às vezes nem é aconselhável. Primeiro, se uma organização (pública ou privada) quer emitir certificados para uso interno, ela obviamente tem o direito de fazê-lo. Qual é o ganho de aderir à ICP-Brasil, cujas exigências de segurança são rígidas demais para muitas organizações, e cujas taxas são altas? Segundo, há a questão de autonomia: várias organizações não querem ou não podem se subordinar a um órgão do Poder Executivo Federal.

E terceiro, a Medida Provisória 2200-2, que criou a ICP-Brasil, inclui um parágrafo (10.2) dizendo que se duas partes concordarem em assinar documentos usando certificados emitidos por uma ICP que não pertence à ICP-Brasil, estes documentos têm valor jurídico.

Ou seja, para uso interno, ou para partes que entram em acordo, não há necessidade de usar a ICP-Brasil.

## 9. ICPs alternativas

Por estes motivos, e por motivos de pesquisa e educação, as universidades brasileiras, lideradas pela UFSC, a Unicamp e a UFMG, estão criando uma ICP independente. Através de um projeto da Rede Nacional de Desenvolvimento e Pesquisa (órgão de pesquisa do MEC e MCT), elas criaram em 2005 a ICP-EDU, uma ICP no âmbito acadêmico, baseada em software livre. A OAB já criou sua própria ICP.

Então, é provável que coexistirão várias ICPs; isto é inevitável. Pela mesma razão que todos nós temos uma grande variedade de carteiras, carteirinhas e cartões, refletindo nossas relações diversas com entidades públicas e privadas, teremos vários certificados diferentes emitidos por ICPs diferentes. Se isso levar a confusão, uma solução seria padronizar as políticas das ICPs por lei, não a imposição de uma única ICP.

## 10. A questão da privacidade

Pessoalmente, não acredito que a idéia de unificar todos esses certificados em um único, emitido pela ICP-Brasil, vá dar certo, porque combinar todos as funcionalidades requeridas por vários órgãos públicos é muito complicado.

Aliás, seria o grande sonho do Grande Irmão, um certificado único por cidadão: pode-se rastrear a vida digital de uma pessoa completamente. Essa questão da privacidade fez vários países desistirem de uma ICP nacional, mas no Brasil ninguém se parece preocupado; ainda não vi nenhuma proposta lidando adequadamente com esta questão.

## 11. Conclusão

Certificação digital é uma tecnologia muito promissora, pois ela permite implementar o não-repúdio e a identificação de pessoas jurídicas e físicas no mundo digital. Mas é uma tecnologia nova, e ainda há bastantes questões tecnológicas, econômicas, jurídicas e políticas a serem resolvidas.

Porém, o maior obstáculo é cultural: estamos todos apegados ao mundo do papel. Uma prova disso é que a primeira imagem que entra em nossa mente quando pensamos na palavra “documento” é a do papel, e não as informações escritas nele. Ou seja, o mundo digital traz uma separação de mídia e conteúdo que no mundo de papel não existia. Ainda mais forte: no caso de uma assinatura de punho, a ligação entre o conteúdo e a assinatura é estabelecida através da mídia; o papel é apenas intermediador, porém essencial na questão da autenticidade e, portanto, da validade jurídica.

Até que todo mundo se acostume ao documento eletrônico e confie na sua autenticidade, vai levar muitos anos, talvez décadas. É uma profunda mudança de paradigma.

# Certificação Digital - Uma Realidade em Minas



## Raymundo Albino

Engenheiro electricista e analista de suporte de sistemas, graduado pela PUC-MG. Atua como assessor técnico da Diretoria de Tecnologia e Produção da Prodemge, tendo passado pela Gerência de Redes e Superintendência de Produção. Participa atualmente do grupo de trabalho criado pelo governador para implantar a certificação digital no âmbito do Estado de Minas Gerais.



## Sérgio Daher

Engenheiro electricista e analista de suporte de sistemas, graduado pela PUC-MG. Atua como superintendente de Tecnologia e Suporte da Prodemge, já tendo exercido diversos cargos gerenciais na empresa. Participa do Grupo de Trabalho de Certificação Digital, instituído pelo Governo do Estado de Minas Gerais.

## RESUMO

O artigo dá uma visão global da necessidade do uso da certificação digital nas instituições, tanto públicas como privadas, especialmente devido ao uso crescente da internet em transações e relacionamentos entre empresas e cidadãos, buscando sempre garantir a Confidencialidade, Integridade e Disponibilidade das informações.

Em seguida, é feita uma explicação sobre conceitos de criptografia, assinatura digital e certificação digital, mostrando as principais aplicações já em uso no Brasil.

O artigo é concluído com a posição da certificação digital no Estado de Minas Gerais, mostrando o que já foi feito e as aplicações já eleitas para utilizarem os benefícios desta tecnologia nos órgãos e entidades estaduais, visando à agilização da máquina administrativa e à melhoria dos processos de relacionamento entre o Estado e o cidadão.

**Palavras-chave:** Certificação Digital (do Estado de Minas Gerais)

Com o crescente aumento de utilização da internet para o trâmite de documentos eletrônicos, verifica-se que as organizações, tanto públicas como privadas, estão cada vez mais preocupadas com a segurança e legalidade desses processos. Quanto à segurança no tráfego

e armazenamento de documentos eletrônicos, os aspectos que mais preocupam as organizações são: sigilo, integridade, autenticidade e não-repúdio. Quanto à legalidade, as preocupações se voltam para a validade jurídica e força probatória. Informações sigilosas são aque-

las que só podem ser acessadas pelo legítimo receptor do documento. A integridade é a garantia de que o documento recebido não está alterado ou fraudado. A autenticidade é a garantia de autoria do emissor ou aprovador do documento. O não-repúdio é a impossibilidade do emissor negar a realização da transação ou autoria. Quanto à legalidade, um documento ou processo eletrônico terá validade jurídica quando aceito como prova e força probatória e quando não puder ser impugnado em uma eventual contestação.

Hoje, a certificação digital, combinando aspectos tecnológicos e jurídicos, possibilita tratar a segurança e legalidade de documentos e processos eletrônicos com garantia de autenticidade, integridade, sigilo, não-repúdio e legalidade. Cresce a cada dia o número de empresas e organizações governamentais que, descobrindo as potencialidades da certificação digital, passam a implementar soluções baseadas nessa tecnologia, aumentando a segurança de seus processos.

## Criptografia

A inviolabilidade de informações sensíveis é uma preocupação constante da humanidade já há muitos séculos. Inúmeros mecanismos de codificação de informações foram

utilizados, com objetivo de reduzir a possibilidade de que adversários obtivessem informações secretas, através da captura de documentos em trânsito ou arquivados.

Historicamente, temos evidências da utilização de mecanismos criptográficos remontando à China antiga. Como exemplo, mostraremos a CIFRA DE CÉSAR, um pouco mais moderna, da época em que Júlio César governava o Império Romano. Este método foi concebido através da substituição posicional do alfabeto, utilizando uma chave que marca o deslocamento a ser adotado na codificação da mensagem. A seguir, mostramos um exemplo onde é utilizada a chave 6, ou seja, cada letra do alfabeto da mensagem original deverá ser substituída pela letra que estiver na 6ª posição anterior, para formar a mensagem cifrada:

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**  
**U V W X Y Z A B C D E F G H I J K L M N O P Q R S T**

**CHAVE = 6**

**ORIGINAL SIGILO PELA CRIPTOGRAFIA**  
**CIFRADA MGACFIUJZ FVUXLCJNIALV CV**

Junto ao desenvolvimento da humanidade, métodos cada vez mais sofisticados foram desenvolvidos, sempre na disputa de uma verdadeira guerra: métodos mais sofisticados de cifragem contra métodos cada vez mais aperfeiçoados de decifragem.

O desenvolvimento da informática tem sido um grande aliado na guerra da criptografia, permitindo que sistemas extremamen-

te complexos de codificação possam ser desenvolvidos, assim como mecanismos de decodificação, também superpoderosos, possam ser concebidos e implementados.

O objetivo é alcançar condições onde mesmo os mais poderosos computadores tenham chances mínimas de decifragem de mensagens em prazos em que métodos administrativos de segurança possam ser implementados a custos razoáveis (troca sistemática de chaves).

O método mais eficaz conhecido é o modelo de chave pública utilizando exponenciação. Cada participante da estrutura possui uma chave secreta e uma chave pública. Assim sendo, uma mensagem, para ser enviada, é inicialmente criptografada pela chave do receptor, garantindo que só ele seja capaz de decifrar a mensagem

através de sua chave secreta. Este processo, utilizando uma chave de duzentos algarismos, dependeria 10 milhões de séculos de um computador capaz de 1 milhão de multiplicações por segundo para que o sigilo fosse quebrado.

O método pode também ser utilizado em sistemas de assinatura eletrônica, quando, então, um documento poderá ser enviado

eletronicamente com garantia de origem e destino.

Apesar da transcrição anterior ser datada de 1992, quando foi publicada na revista comemorativa dos 25 anos da Prodemge, época ainda anterior à realidade atual do mundo Web, demonstra-se atual nas técnicas da segurança da informação.

O que ocorreu nos anos que se seguiram foi a massificação da sua utilização através das aplicações de comércio eletrônico, hoje utilizado por toda a comunidade conectada à internet, seja para a compra de mercadorias e serviços, ou mesmo a consulta do saldo de uma conta corrente bancária através da Web.

O estágio atual da utilização das técnicas de criptografia no ambiente das transações eletrônicas se resume, na grande maioria das aplicações, à garantia da autenticidade do destino a que se conecta o usuário, assegurando-lhe que a instituição, na qual uma determinada transação está sendo efetuada, seja aquela que ele realmente deseja e espera, preservando também o sigilo das comunicações trocadas durante o procedimento.

O que nos avizinha é a identificação inequívoca também do usuário dos sistemas de informação, obtida através de certificados digitais pessoais, seja de pessoas físicas ou jurídicas, garantindo, desta forma, a impossibilidade do repúdio da realização das transações por elas originadas.

Tal realidade, em um futuro próximo, trará garantias adicionais a toda a comunidade envolvida com o mundo das transações eletrônicas, destino inexorável de toda a civilização.

# Sistema de Criptografia RSA

## O receptor da mensagem:

- > escolhe dois números primos,  $p$  e  $q$ , calculando  $n=p \cdot q$ ;
- > determina  $\phi(n) = (p-1) \cdot (q-1)$ ;
- > escolhe o expoente de codificação, tal que  $1 < e < \phi(n)$  e  $\text{mdc}(e, \phi(n)) = 1$ ;
- > determina o expoente de decodificação, tal que  $1 < d < \phi(n)$  e  $ed = 1 \pmod{\phi(n)}$ ;
- > publica o par  $(n, e)$ , que se diz a Chave Pública, mantendo secreto o par  $(n, d)$ , a Chave Privada.

## O emissor da mensagem:

- > converte a mensagem no número inteiro  $M$ ,  $0 < M < n$ , recorrendo a um "alfabeto digital", por exemplo,  $A = 01$ ,  $B = 02$ ,  $C = 03$ , ...,  $Z = 26$ ;
- > obtém a chave pública  $(n, e)$  do destinatário;
- > converte o número  $M$  no número  $C$  através da fórmula de codificação:  
 $C = M^e \pmod{n}$ , onde  $M$  representa a mensagem original e  $C$  a mensagem codificada;
- > envia a mensagem  $C$ , ao destinatário.

## O receptor da mensagem:

- > determina o inteiro  $M'$  usando a fórmula de decodificação  $M' = C^d \pmod{n}$ ;
- > como  $M' = M$ , recorre ao "alfabeto digital" e obtém a mensagem original.

## Exemplo:

### Determinação das chaves

- > Primos  $p=11$  e  $q = 23$ ;  $n = 11 \times 23 = 253$ , e  $\phi(n) = (11 - 1)(23 - 1) = 10 \times 22 = 220$ .
- > Como  $\text{m.d.c.}(3, 220) = 1$ , o expoente de codificação é  $e = 3$ .
- > Como  $3d = 1 \pmod{220}$  -  $d = 147$ , o expoente de codificação é  $d = 147$ . Assim, a chave pública é  $(253, 3)$  e a chave privada é  $(253, 147)$ .

### Codificação da mensagem SOL

- > Recorrer-se a um "alfabeto digital":  $M = 191512$ .
- > Como  $M > n = 253$ , divide-se  $M$  em blocos  $M_1 = 19$ ,  $M_2 = 15$  e  $M_3 = 12$ .
- > Usando a chave pública  $(253)$ , efetua-se a codificação de cada um dos blocos:  $19^3 = 6859 = 28 \pmod{253}$ ,  $15^3 = 3375 = 86 \pmod{253}$  e  $12^3 = 1728 = 210 \pmod{253}$
- > A mensagem codificada é  $C = 2886210$ .

### Decodificação da mensagem

- > Usando a chave privada,  $(253, 147)$ , tem-se:  $28147 = 19 \pmod{253}$ ,  $86147 = 15 \pmod{253}$  e  $210147 = 12 \pmod{253}$
- > Portanto,  $M' = 191512 = M$
- > Conhecido o número  $M$ , basta recorrer ao "alfabeto digital" para obtermos a mensagem inicial: SOL.

## Assinatura Digital

Logicamente, nos dias de hoje, cifras tão simples como a Cifra de César, e até mesmo aquelas mais complexas utilizadas antigamente, seriam facilmente quebradas pelo uso de computadores, através de um método denominado "força-bruta", onde são realizadas tentativas sucessivas até se chegar à chave desejada.

A criptografia moderna, essencial para a segurança de computadores conectados em rede, especialmente à internet, consiste em algoritmos complexos, de forma a dificultar ao máximo a ação de invasores.

As funções de criptografia aplica-

das aos computadores podem ser divididas em duas categorias: *criptografia* e *autenticação*.

## Criptografia

O ato de criptografar, conforme já abordado e detalhado a seguir, se refere ao embaralhamento das informações de uma mensagem, de forma que alguém sem autorização não possa compreendê-la.

## Autenticação

Já a autenticação é o procedimento para verificação de autenticidade do emissor da mensagem. Para realizar uma autenticação, é necessário proteger a mensagem de forma que ela não

seja modificada, o que é normalmente feito através da incorporação de uma *assinatura digital*.

Tipicamente, uma assinatura é formada pela utilização de uma função denominada *hash*, que consiste no cálculo e codificação de um resumo da mensagem completa, formando um código de tamanho fixo que é cifrado e transmitido junto com a mensagem original, garantindo a autenticidade da mensagem.

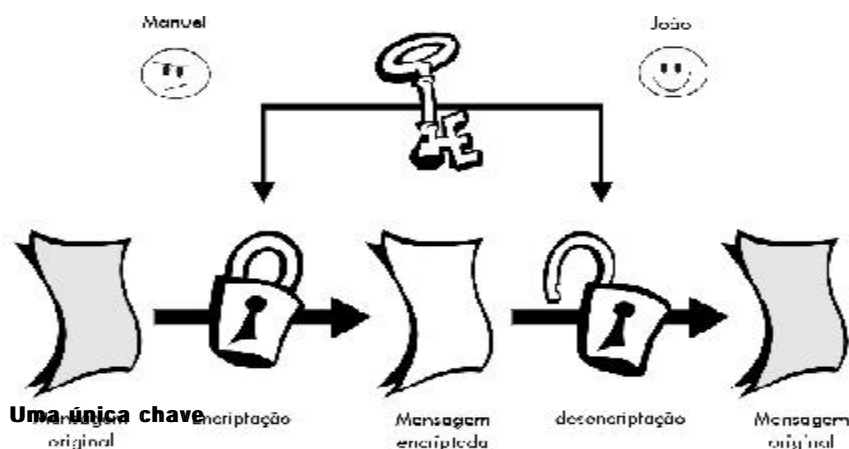
Podemos dividir as técnicas de criptografia em dois tipos básicos: Criptografia Simétrica ou de Chave Privada, onde uma única chave é utilizada para criptografar e decifrar, e Criptografia Assimétrica ou de Chave Pública, onde é usado um par de chaves



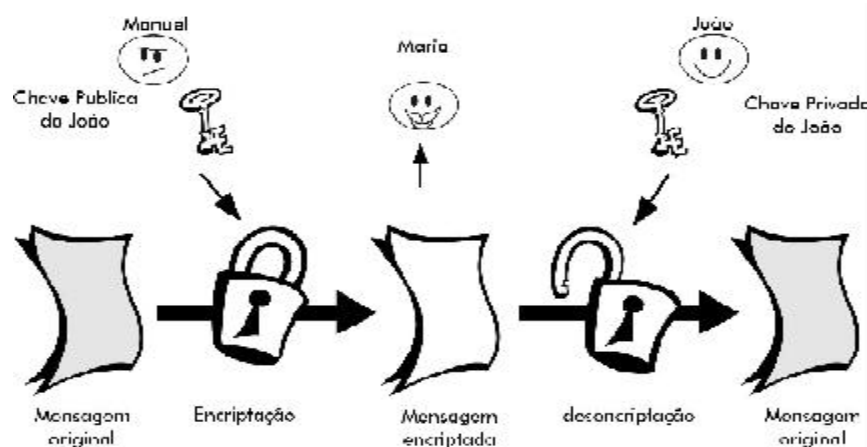
relacionadas entre si, que são a chave pública e a chave privada. As técnicas de criptografia simétricas mais conhecidas são a DES e a AES. O RSA é o algoritmo assimétrico mais conhecido.

## Tipos de Criptografia

### \* Criptografia Assimétrica ou de Chave Pública



### \* Criptografia Simétrica ou de chave secreta



**Duas chaves:** - chave pública, que é publicada;  
- chave privada, que é mantida secreta.

No âmbito da certificação digital, a modalidade mais utilizada é a denominada híbrida, como o protocolo SSL, que utiliza a criptografia assimétrica na inicialização de uma sessão Web, quando é trocada uma chave simétrica, tipo DES, que será utilizada no transcorrer da sessão já iniciada, até o seu término, quando então é descartada.

Tal procedimento visa a alcançar o máximo de segurança - porque a chave simétrica é utilizada apenas uma vez, sendo que ela é gerada dinamicamente, a cada sessão estabelecida - aliado ao mínimo de processamento necessário nos computadores envolvidos. Assim, o algoritmo DES consome menos recursos computacionais quando comparado ao algoritmo RSA utilizado na criptografia assimétrica, ou de chave pública.

Para realizar a assinatura de documentos, é necessária a utilização de um par de chaves, sendo que o emissor assina o documento com sua

chave privada, e o receptor deverá possuir a chave pública do emissor para que possa ser comprovada a autenticidade do documento.

Já no caso de emissão de documento sigiloso criptografado, o procedimento é o oposto, ou seja, o emissor deverá possuir a chave pública do receptor, de forma que somente ele, ao receber o documento, poderá decifrá-lo com a sua chave privada.

No caso de documentos assinados e criptografados, deverão ser seguidos os dois procedimentos anteriormente citados em conjunto.

É importante salientar a diferença entre assinatura digital (explicada acima) e assinatura eletrônica, que pode ser, por exemplo, um e-mail transmitido em claro, o qual não possui garantia de autenticidade.

A geração de um par de chaves está demonstrada no quadro da página ao lado.

## Certificação Digital

A certificação digital é o procedimento que utiliza um arquivo eletrônico que acompanha um documento assinado de forma digital, cujo conteúdo é criptografado. Este documento é denominado *certificado digital* e contém informações que identificam a pessoa e/ou computador com que se está tratando na rede. Um documento eletrônico que possui certificação digital tem garantia de autenticidade de origem e autoria, de integridade de conteúdo, de confidencialidade e de não-repúdio, ou seja, de que a transação, depois de efetuada, não poderá ser negada pela parte que

utilizou a certificação.

O certificado digital é uma credencial eletrônica definida de acordo com o padrão ITU-T X.509, e é emitido por uma Autoridade Certificadora (terceiro de confiança) que garante a identidade do portador / usuário de forma análoga a uma Carteira de Identidade.

A Autoridade Certificadora - AC- e a Autoridade de Registro - AR- são entidades de confiança responsáveis pela emissão dos certificados, bem como pela manutenção de toda a estrutura vinculada à certificação digital dentro de seu âmbito de atuação. Dentro da ICP-Brasil, as ACs e ARs estão credenciadas em uma estrutura hierárquica, que tem uma *Chave Raiz* responsável pela geração das Chaves Secundárias, que por sua vez emitem os certificados de usuários.

As aplicações de certificação digital podem ser divididas em duas categorias que são a certificação pessoal e a certificação de servidores.

#### > Certificação Pessoal

- A certificação pessoal refere-se aos certificados emitidos em nome de uma pessoa natural ou jurídica, de forma a identificá-la inequivocamente, ou seja, a pessoa, ou o representante legal da entidade, associada àquela pessoa jurídica.

Tais certificados são utilizados na assinatura de mensagens eletrônicas, bem como no relacionamento dessas pessoas com os aplicativos que exigem a identificação segura de seus usuários.

#### > Certificação de Servidores

- A certificação de servidores se destina à identificação de serviços ou grupos de serviços associados a uma determinada URL primária, Uniform Resource Locator, que é o identificador mundial de documentos e demais recursos na internet, ou seja, todas as URLs derivadas de um determinado endereço eletrônico de um servidor.

Este mecanismo garante que as informações obtidas se originam verdadeiramente daquele endereço certificado, a exemplo dos bancos e demais aplicações que requerem segurança da informação.

São exemplos bem-sucedidos de utilização de certificação digital no Brasil:

- o e-CPF e o e-CNPJ na Secretaria da Receita Federal, que possibilitam o relacionamento seguro via internet dos contribuintes com a instituição para acesso de informações não disponíveis de forma convencional;

- o processo de tramitação eletrônica de documentos oficiais, que serão publicados no Diário Oficial da União, utilizado pelo Presidente e seus ministros, que possui um sistema que faz o controle do fluxo de forma automática, garantindo segurança, agilidade e eficiência;

- o Sistema de Escrituração Fiscal da Secretaria da Fazenda do Estado de Pernambuco, que obriga que os lançamentos de registro de operações e prestações relativas ao ICMS sejam feitos através de arquivo eletrônico assinado de forma digital, que incorpora uma série de benefícios, tais como: entrega de vários documentos em uma única remessa, redução drástica no volume de

erros de cálculo involuntário, eliminação de múltiplas escriturações, redução de custos de escrituração e armazenamento de livros fiscais, etc.;

- sistema de encaminhamento de Petições Eletrônicas no TRT-4 do Rio Grande do Sul, agilizando o tempo de cada processo de forma segura e econômica;

- o sistema PUBNet da Imprensa Oficial de São Paulo, que automatiza por completo todo o ciclo de publicações na internet de forma segura e rápida, evitando-se congestionamentos telefônicos anteriormente registrados com constância. Também foi possível, através do uso da certificação digital, a criação do e-diário oficial, que é o Diário Oficial em formato eletrônico.

#### Certificação Digital no Estado de Minas Gerais

Recentemente, a administração pública estadual identificou a necessidade de automatizar determinados processos de tramitação de documentos em sua esfera, necessitando, portanto, de ferramentas capazes de, eletronicamente, controlar o fluxo dos documentos com segurança, garantia de autenticidade e autoria, bem como com garantia de sigilo em determinados processos protegidos pela legislação em vigor.

Com base em tais requisitos, optou-se, como não poderia deixar de ser, por tecnologias envolvendo certificados digitais para pessoas físicas e jurídicas, em suas interações com o poder público estadual.

Foram consideradas as possibilidades existentes no mercado

como a criação de uma infra-estrutura de chaves públicas (ICP) estadual, baseada em certificados digitais próprios do Estado, bem como a sua adesão à ICP-Brasil.

Essa adesão foi decidida em função da garantia de validade jurídica nos relacionamentos eletrônicos conforme disposto no texto da Medida Provisória 2.200-2, bem como pelos fatores técnicos de segurança, já que a ICP-Brasil possui regras rígidas para credenciamento, com auditorias regulares, aumentando, dessa forma, a credibilidade dos certificados emitidos.

Avaliando-se as várias alternativas técnico-econômicas apresentadas, optou-se pela adesão do Estado à ICP-Brasil, por intermédio da contratação de uma autoridade certificadora de primeiro nível, ou seja, diretamente subordinada à raiz da ICP-Brasil, que terceirizaria as atividades relacionadas à infra-estrutura de segurança necessária ao desempenho das funções relacionadas à emissão dos certificados, bem como pela guarda da chave primária da AC estadual.

Através da instauração de um grupo de trabalho específico para deliberar sobre o assunto, ficou determinado que seria a Prodemge a Autoridade Certificadora do Estado.

Através de um processo licitatório, a Prodemge contratou a empresa Certisign como a provedora da infra-estrutura necessária. Cumpridas as determinações do ITI, foi publicado o Despacho da entidade, reconhecendo formalmente a Prodemge como Autoridade Certificadora e Autoridade de Registro, dentro dos padrões

da ICP-Brasil.

Várias iniciativas estão em curso no Estado para a utilização de certificados digitais em aplicações do Governo de Minas Gerais, principalmente aquelas que possibilitem a desburocratização dos procedimentos usuais das empresas e cidadãos nos seus relacionamentos com o Estado.

Podemos destacar, entre essas iniciativas, as seguintes:

- tramitação segura de documentos (Workflow) entre os diversos segmentos governamentais, garantindo maior agilidade, segurança e redução de custos pela diminuição da burocracia;

- digitalização / Gestão Eletrônica de Documentos da Junta Comercial do Estado de Minas Gerais, propiciando uma redução expressiva de documentos, aumentando a segurança e reduzindo o tempo de acesso às informações armazenadas;

- registro eletrônico de alterações contratuais via Web na Junta Comercial do Estado de Minas Gerais, aumentando a segurança, reduzindo o tempo de atendimento e a necessidade de deslocamentos ao local;

- relacionamento seguro, através de certificados, da Secretaria da Fazenda do Estado de Minas Gerais com contribuintes de ICMS, possibilitando o envio e consultas de informações de forma segura e identificada;

- relacionamento seguro de fornecedores do Estado, agilizando os processos de compras e aquisições, em especial com a Secretaria de Planejamento e Gestão, responsável por um volume sig-

nificativo de licitações;

- relacionamento seguro dos servidores estaduais com as diversas instituições, em especial com a Secretaria de Estado de Planejamento e Gestão e o Instituto de Previdência Estadual, possibilitando maior agilidade no atendimento, com redução de custos devido a um maior controle;

- identificação segura dos usuários de sistemas corporativos computadorizados, garantindo segurança e transparência nas atividades do Estado;

- comercialização segura de documentos sob responsabilidade da Imprensa Oficial do Estado de Minas Gerais;

- utilização de correio eletrônico com assinatura por todos os servidores estaduais.

As melhorias incorporadas, com a utilização da certificação digital, nos diversos aplicativos existentes ou em desenvolvimento no Estado de Minas Gerais adicionarão celeridade aos diversos processos, bem como trarão ainda maior transparência às ações da administração pública estadual.

Necessária. Cumpridas as determinações do ITI, foi publicado o Despacho da entidade, reconhecendo formalmente a Prodemge como Autoridade Certificadora e Autoridade de Registro, dentro dos padrões da ICP-Brasil.

**Caro Leitor,**

Há alguns meses, quando decidimos lançar uma revista técnica, com a chancela da Prodemge, estabelecemos de imediato um compromisso: criar uma publicação relevante, que tivesse um destino outro que enfeitar mesinhas de ante-salas de repartições. O maior temor num projeto como esse era de que, depois de pronto, soasse como uma mera reverência às vaidades de uma estatal que atua no ramo da tecnologia.

Definimos então, como premissa editorial, a concentração exclusiva em temas que estivessem na ordem do dia dos usuários, atuais ou potenciais, da tecnologia da informação. Além disso, a abordagem deveria buscar o tom exato entre a profundidade e a leveza. A primeira, deveria torná-la referência de pesquisa para usuários, técnicos e executivos em busca de conhecimentos para ajudá-los em suas decisões e estudantes em busca da última palavra sobre os temas em pauta. A segunda, cuidaria de que fosse uma publicação agradável, rica e informativa, capaz de despertar também a atenção do público interessado, mas não especializado, importante já que numeroso e formador de opinião.

Este primeiro número de Fonte reflete bem essas diretrizes.

O tema não poderia ser mais atual: Certificação Digital.

É assunto novo, com vastas áreas ainda em discussão, e que certamente provocará, em futuro próximo, profunda revolução nos costumes da sociedade em geral e, principalmente, na administração pública, com reflexos simplificadores sobre a vida dos cidadãos. Abordamos todos os seus aspectos: os legais, os técnicos, os administrativos e os culturais. Buscamos como colaboradores as maiores autoridades em cada setor, que contribuíram com entrevistas exclusivas ou textos inéditos. Procuramos, sem a pretensão de esgotar o assunto, refletir o panorama mais atual do estágio em que se encontram as discussões sobre o tema no País.

Temos a consciência de que o que apresentamos agora não é um produto acabado. Por isso, abrimos uma seção para interação com os leitores. Dela, tiraremos sugestões, ouviremos críticas e, eventualmente, buscaremos inspiração para possíveis e oportunas correções de rumo.

Finalmente, analisando este primeiro número de Fonte, que agora publicamos, temos a esperança de termos escapado da irrelevância.

No entanto, submetemos esta avaliação ao julgamento soberano - na realidade o que realmente importa - dos nossos leitores.

Um abraço,

**Maurício Azeredo Dias Costa**

Uma Publicação da:



Ano 1 - nº 1 - Dezembro de 2004

**Governador do Estado de Minas Gerais**  
Aécio Neves da Cunha  
**Secretário de Estado de Planejamento e Gestão**  
Antonio Augusto Junho Anastasia  
**Diretor-Presidente**  
Maurício Azeredo Dias Costa  
**Diretora de Projetos e Negócios**  
Glória Maria Menezes Mendes Ferreira  
**Diretor de Tecnologia e Produção**  
Raul Monteiro de Barros Fulgêncio  
**Diretor Administrativo e Financeiro**  
José Ronaldo Fidelis  
**Diretor de Desenvolvimento Empresarial**  
Nathan Lerman

## Fonte

### CONSELHO EDITORIAL

Antonio Augusto Junho Anastasia  
Maurício Azeredo Dias Costa  
Márcio Luiz Bunte de Carvalho  
Amílcar Vianna Martins Filho  
Gustavo da Gama Torres  
Paulo Kléber Duarte Pereira  
Marcos Brafman

### EDIÇÃO EXECUTIVA

Assessoria de Comunicação  
Pedro Marcos Fonte Boa Bueno  
Edição, reportagem e redação  
Isabela Moreira de Abreu - MG 02378 JP  
Coordenação do projeto editorial, gráfico e publicitário  
Gustavo Grossi de Lacerda  
Universidade Corporativa Prodemge  
Enilton Rocha Ferreira  
Marta Beatriz Brandão P. e Albuquerque  
Luiz Cláudio Silva Caldas  
Projeto gráfico, capa, ilustrações, diagramação  
e editoração gráfica  
Guydo José Rossi Cardoso de Menezes  
Estágio programação visual  
Camila Maciel Leite Seabra  
Revisão  
Fátima Campos  
Fotolito e impressão  
Policron / Gráfica Formato  
Tiragem  
Três mil exemplares  
Periodicidade  
Semestral

### PATROCÍNIO

Esta edição da revista contou com o apoio:



**Prodemge - Rua da Bahia, 2277 - Bairro Lourdes  
CEP 30160-012 - Belo Horizonte, MG, Brasil**  
[www.prodemge.mg.gov.br/](http://www.prodemge.mg.gov.br/) / [prodemge@prodemge.gov.br](mailto:prodemge@prodemge.gov.br)



**Fonte**

---

# Sumário

---

**Fonte**

Número 01 - Dezembro de 2004

**prodemge**

Tecnologia de Minas Gerais

---

- 03** **Interação:** comentários e sugestões de leitores
- 04** **Diálogo:** entrevista com o advogado-geral do Estado de Minas Gerais, José Bonifácio Borges de Andrada, que fala dos aspectos histórico e jurídico da certificação digital no País
- 11** **ICP-Brasil: Evolução com Equilíbrio e Correção** - o diretor do ITI, Evandro Oliveira, aborda o comportamento do mercado frente à consolidação da certificação digital
- 13** **Governo Eletrônico: Projeto de Segurança da Informação do Governo Mineiro** - a secretária-adjunta de Planejamento e Gestão do Governo do Estado de Minas Gerais, Renata Vilhena, comenta o desafio da segurança da informação com o uso crescente da tecnologia
- 14** **A Criptografia na Ficção** - técnicas antigas e fantasias modernas no artigo do analista de sistemas da Prodemge, Luís Carlos Silva Eiras
- 16** **Dossiê:** panorama da certificação digital - aplicações, benefícios, perspectivas e a opinião de autoridades no assunto
- 32** **Benchmarking:** duas experiências de sucesso - a Receita Federal e o Tribunal Regional do Trabalho 4ª Região (RS)
- 35** **Fórum:** a certificação digital e os cartórios - o professor de Ciência Política, José Eisenberg, comenta o desafio que a certificação digital representa para o futuro da burocracia
- 37** **Universidade Corporativa Prodemge:** seleção de artigos acadêmicos inéditos sobre os temas certificação digital e segurança da informação
- Considerações sobre a interoperabilidade aplicada à infra-estrutura de chaves públicas - Fabiano Menke
- A privacidade na ICP-Brasil - Alexandre Rodrigues Atheniense
- Tudo que você deve saber sobre certificação digital - Jeroen van de Graaf
- Certificação digital: uma realidade em Minas - Raymundo Albino e Sérgio Daher



---

# Interação

---

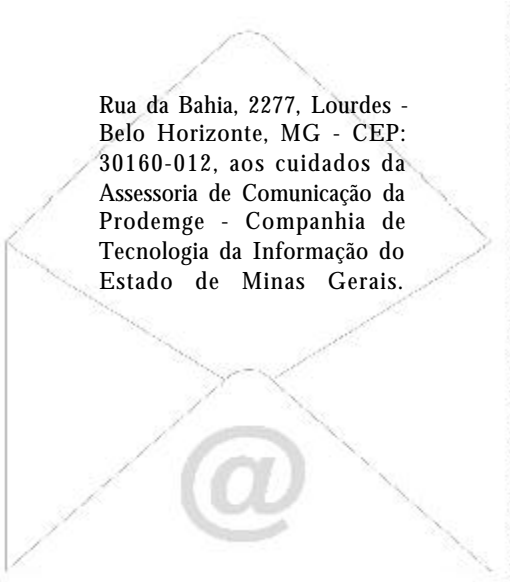
Este espaço é  
destinado a acolher  
as opiniões e  
sugestões de  
nossos leitores.

Participe, contribua,  
faça contato:  
seu retorno é  
fundamental para  
que a  
revista evolua a cada  
edição.

---

**e-mail:**  
**[revistafonte@prodemge.gov.br](mailto:revistafonte@prodemge.gov.br)**

---



Rua da Bahia, 2277, Lourdes -  
Belo Horizonte, MG - CEP:  
30160-012, aos cuidados da  
Assessoria de Comunicação da  
Prodemge - Companhia de  
Tecnologia da Informação do  
Estado de Minas Gerais.

### Segurança e armazenamento de documentos: da inscrição na pedra à Certificação Digital



**José Bonifácio Borges de Andrada, advogado-geral do Estado/MG. Dentre os vários cargos públicos que exerceu, foi advogado-geral da União, subsecretário-geral da Presidência da República, secretário-executivo do Ministério da Justiça, subchefe para assuntos jurídicos da Casa Civil da Presidência da República e consultor jurídico do Ministério da Previdência e Assistência Social. Tem o cargo efetivo de procurador regional da república.**

Na primeira edição da Revista Fonte, o entrevistado é o advogado-geral do Estado, José Bonifácio Borges de Andrada. Com larga experiência no setor público, no qual ocupou importantes cargos nos governos Federal e Estadual, e também com grandes conhecimentos na área de tecnologia da informação, o advogado-geral do Estado teve participação decisiva na criação da Infra-Estrutura de Chaves Públicas do Brasil – ICP-Brasil, atuando primeiramente como consultor jurídico do Ministério da Previdência e Assistência Social, onde surgiram as primeiras evidências da necessidade de mecanismos de proteção às informações eletrônicas; e, posteriormente, como subsecretário-geral da Presidência da República e advogado-geral da União, quando foi finalmente estabelecida a Medida Provisória 2200, que regulamenta a certificação digital no Brasil.

Nesta entrevista, José Bonifácio traça, de forma didática, um panorama histórico da certificação digital no País e fala, com propriedade e bom humor, das perspectivas dessa tecnologia no Brasil. Ele refuta o mito de seu uso explosivo no comércio eletrônico e pontua os benefícios de sua utilização para o setor público, enfatizando a experiência em Minas, onde a tecnologia tornou-se realidade em 2004.

**Fonte: Como surgiram as primeiras iniciativas para estabelecer o serviço no Brasil?**

“Eu fui despertado para essas questões de informática, do ponto de vista legal, quando trabalhava no Ministério da Previdência. Algumas fraudes vinham sendo feitas no sistema ou através do sistema. Algumas, muito primárias, muito simples; outras, devido à falta de cuidado de pessoas que deixavam seu cartão magnético com a senha pregada com durex na tela do computador, para facilitar o serviço. Havia no entanto outras mais complexas, mais elaboradas, que exigiam um pouco mais de conhecimentos. Houve um dia em que um hacker conseguiu fazer clone da página da Previdência e colocou informações para confundir as pessoas. A nossa sorte é que ele colocou um Fale Conosco. Mandamos então um e-mail para ele, dizendo que a Polícia estava chegando. Conseguimos resolver o problema e tirar a falsa página do ar.

Com esses episódios, chegamos à conclusão de que era necessária uma legislação criminal específica para a área previdenciária. Elaboramos então algumas alterações no Código Penal, que estão em vigor hoje, para a proteção da base de dados da Previdência. Esse projeto foi encaminhado ao Congresso. Nesse meio tempo, eu fui convidado para trabalhar na Casa Civil e o projeto tramitava no Congresso.

Na Casa Civil, nós temos um contato maior com a estrutura de Governo e começamos a perceber que a demanda era comum a todos os outros órgãos.”

**Fonte: Naturalmente, houve necessidade de adequações na Lei. Como foi conduzido o processo?**

“Percebemos que todos os órgãos tinham dados e informações que precisavam ser preservados e que o projeto da Previdência, que estava mais avançado, na verdade servia para todo mundo. Fizemos então algumas alterações no Projeto de Lei que estava na Câmara e o adequamos para a administração pública. Foram então criados, pela primeira vez, alguns crimes específicos, que estão no Código Penal. Isso é importante também: não fizemos uma lei específica, fizemos alterações no Código Penal, que é a lei penal comum, que todo mundo usa, a lei básica criminal do País, protegendo documentos e informações constantes em bases de dados e também criando algumas hipóteses criminais de invasão de bases de dados.

Por exemplo, ceder senha de acesso a um banco de dados protegido a um terceiro, em certos casos, é crime. Uma pessoa não pode passar informalmente a senha a uma pessoa não autorizada. Só passar a senha já é crime. Se isso significa uma invasão a uma base de dados, é um outro crime com pena mais grave. Se, da invasão, resulta um dano à base de dados, aí é outro crime, com pena mais alta ainda. Não estávamos ainda na fase da certificação digital. Mas chegou-se a um ponto em que houve demanda pela certificação digital.”

**Fonte: Nessa época, como outros países conduziam a questão da segurança de seus documentos eletrônicos?**

“Nessa época, ou um pouquinho antes, a Europa já tinha feito uma diretriz para a União Européia. Uma diretriz básica que orientava todos os países sobre como regulamentar a certificação digital na Europa.

Outros países também estavam fazendo uma legislação própria. Nos Estados Unidos, bem no seu estilo – devido à liberdade de cada Estado –, cada um definia

**“Foram estudados os modelos do mundo e o governo optou por adotar o modelo vigente na Comunidade Européia...”**

sua forma de atuação mais conveniente. Mas o assunto estava em fase de organização, por volta de 1999/2000.

E nós sentimos a necessidade de que houvesse aqui no País também alguma forma de regulamentação. Nós, da área jurídica, conhecíamos pouco sobre o assunto; tivemos que estudar, porque não conhecíamos, naturalmente, a legislação, a prática e os mecanismos de funcionamento da certificação digital. Tivemos que nos informar, estudar muito, contando com a ajuda de especialistas. O professor Miguel

Teixeira Carvalho, do Ministério da Ciência e Tecnologia na época, e o pessoal do Serpro nos ajudaram muito no entendimento da certificação digital e os conceitos de chave pública, chave privada, algoritmo de hash e outros. E, ao entender a certificação digital, tivemos também que entrar no conceito de Autoridade Certificadora e Autoridade Raiz, o que foi muito importante para depois estabelecer o modelo.”

**Fonte: O senhor participou ativamente da concepção da ICP-Brasil, ajudando a definir o modelo de certificação que foi adotado no País. Como foi feita essa escolha?**

“O modelo de certificação digital que o Brasil adotou está na Medida Provisória 2200. Foram estudados os modelos do mundo e o Governo optou por adotar o modelo vigente na Comunidade Européia, previsto na Diretiva 93/1999, por dois motivos: primeiro, devido à similitude da legislação – a nossa legislação é uma herança do sistema romano-germânico, nossas leis são baseadas nas leis portuguesas, espanholas, italianas, e sofrem muita influência do direito alemão. A maneira de legislar brasileira, a nossa maneira de agir no processo judicial, é muito mais próxima do sistema europeu. Chegamos à conclusão de que seria, portanto, mais fácil para o mundo jurídico brasileiro assimilar, com mais rapidez, um conjunto de normas que tivesse uma sistemática européia do que uma sistemática americana.

O segundo motivo é que a sistemática européia é compatível com a sistemática americana, mas o contrário não ocorre. Se

adotássemos o modelo europeu, o sistema brasileiro conversaria com os americanos; mas se adotássemos o modelo americano, teríamos dificuldades para conversar com os europeus. É que a Diretiva Européia 93/1999 dá padrões mínimos básicos de organização do sistema, mas, ao mesmo tempo, ela tem que ser flexível o suficiente para respeitar as diversidades culturais de cada país. A Diretiva, portanto, não poderia ser muito rígida.

Resumindo, as coisas funcionam mais ou menos assim: na medida em que nós respeitamos a Diretiva Européia, passamos a ser como “um membro da comunidade europeia”. Se os sistemas dos vários países falam entre si, falam também com o nosso. Isso, para negociações futuras, facilita nosso ingresso na Europa; e o sistema americano é absolutamente aberto, na realidade, aceita qualquer um.”

### **Fonte: O que exatamente determina a Medida Provisória 2200?**

“A opção do Governo está sintetizada na MP-2200, que prevê dois sistemas paralelos, que operam simultânea e livremente: um sistema de certificação livre e um sistema de certificação governamental.

Para este, foi criada a Autoridade Raiz única – que é o ITI –, uma autarquia federal, a Infra-Estrutura de Chaves Públicas hierarquizada, dentro da estrutura da ICP. A MP estabeleceu ainda que a Autoridade Raiz não tem contato com o usuário, quer dizer, ela não é a fornecedora do certificado no nível do usuário; ela certifica as autoridades certificadoras de segundo nível, que

podem ser órgãos públicos ou privados. Ou seja: a MP criou o modelo da infra-estrutura e fixou as atribuições legais do sistema público e privado, copiando rigorosamente a Diretiva Européia.”

### **Fonte: Faça, por favor, um paralelo entre uma operação apoiada pela ICP-Brasil e uma feita fora dessas regras.**

“Em pouquíssimos casos, há a obrigatoriedade de se trabalhar com a autoridade pública. Na prática, é o seguinte: se você trabalha com a ICP-Brasil e assina um documento eletrônico, você não pode negar que assinou o documento. E a parte do outro lado tem o direito de presumir que você o assinou. Se você quiser dizer que aquele documento não foi assinado por você, você tem que fazer a prova. É a presunção de autoria. É uma operação mais segura, porque equivale a uma operação com testemunhas. A Autoridade Raiz e a Autoridade Certificadora são testemunhas de que você é você – o Governo certifica que você é você e a Lei presume que você é o autor do documento.

Fora da ICP, acontece o contrário: se a outra parte duvidar da autoria, cabe ao emitente provar a autenticidade de sua assinatura. As operações são mais tranquilas e mais rápidas porque a outra parte aceitará a sua assinatura se quiser; se não quiser, ela não concorda que você assinou e não faz a operação. E se ela questionar a sua assinatura, você é que tem que provar que ela é autêntica.

Fora da ICP, você não terá uma autoridade: você terá uma

testemunha privada que as partes aceitarão se e na medida em que quiserem. Por exemplo, duas empresas podem contratar uma certificadora privada e fazer negócios, sem problema nenhum, fora da PKI ou ICP oficial.”

### **Fonte: Na prática, como o mercado assimilará esses dois sistemas paralelos?**

“Eu acredito que será o seguinte: na maioria das operações comerciais de baixo valor, você não usará certificação nenhuma, permanecerá como está funcionando atualmente, com cartões de crédito, por e-mail por exemplo. Eu não vou querer comprar um cartão de certificação para isso. E o entregador de gás ou pizza também vai continuar da mesma forma. A certificação seria um custo a mais.

Para as operações de porte médio, eventualmente as empresas vão contratar infraestrutura particular. Não será necessário entrar na esfera governamental, que é mais cara porque a segurança é maior. Se você não precisa de muita segurança, não há motivo para aumentar o custo.

Agora, para documentos oficiais, para os quais a Lei exige autenticidade, aí, nesses poucos casos, você será obrigado a entrar no sistema da ICP-Brasil; ou ainda se o valor das operações for muito alto ou se, por segurança, as partes optarem também pela ICP-Brasil. E as empresas certificadoras também têm inteira liberdade. A mesma empresa pode oferecer serviços dentro da ICP e fora da ICP.

O que vai acontecer é que a certificação emitida pela ICP-

Brasil vai custar mais caro; fora do sistema, a empresa não vai precisar pagar taxas por esse documento, não é submetida à fiscalização e não é exigido dela um certo padrão de qualidade, como a ICP-Brasil, que tem padrão internacional. A nossa Autoridade Raiz – que é o ITI – tem que estar e está no mesmo padrão de qualidade da Europa.”

**Fonte: Comente a certificação digital como solução para a questão da segurança. Como esse expediente se contrapõe ao uso do documento em papel?**

“No fundo, nós convivemos com o uso da correspondência eletrônica em grande escala: hoje, você troca muito e-mail, muita correspondência por computador. Além do e-mail, há também o sistema de mensagem direta, que são os messengers, e o sistema de imagem também – brevemente a certificação vai ter que contemplar a imagem. Daqui a pouco, você vai ter a conversa na internet com som e imagem, gravá-los em CD e com possibilidade de certificação do CD.

A partir de um determinado momento, a comunicação pela internet perde a confiabilidade. Isso acontece mais ou menos como com o telefone e com o fax. Ninguém compra, por exemplo, uma casa por telefone. Tanto vendedor quanto comprador vão querer tudo bem escrito, documentado, com testemunhas, em cartório. Há o serviço de telepizza – por telefone –, mas não há o telecasa. Há vários serviços de comércio por telefone. Mas algumas operações, a partir de um certo valor, você não vai fazer por telefone. Você vai querer se certificar da operação.

Em geral, a certificação se faz em papel: você faz um contrato, busca testemunhas, registra em cartório. Na verdade, a certificação digital não se dirige para a grande massa de operações comerciais. É um engano achar isso. Funciona da mesma forma que a certificação em papel, que você faz para operações de grandes valores, duradouras. Assim como você não faz a compra de uma casa ou apartamento, por telefone, você também não faz uma escritura pública para comprar um sanduíche. Ali é importante justamente que não tenha a certificação. Porque ela torna o

**“Na verdade, a certificação digital não se dirige para a grande massa de operações comerciais. É um engano achar isso.”**

processo mais lento e, nos negócios de grande escala, de pequeno valor unitário, você quer velocidade, e a certificação vai atrapalhar isso. A relação custo–benefício faz valer a pena o risco.

Para ilustrar: quando você pede uma entrega de gás, por telefone, você pode estar falando com o Jack, o Estripador. Há uma possibilidade mínima de não ser o entregador de gás. Da mesma forma que o rapaz do gás pode estar recebendo o telefonema do Jack, o Estripador. Se, toda vez que se fizer uma operação dessa natureza, for exigido documento de identidade, ou outros, ele não vai vender nenhum botijão de gás.

Ele, portanto, tem que correr algum risco.

Isso vale, da mesma forma, para a compra de uma passagem aérea pela internet: você quer facilidade, velocidade, portanto, não se usa a certificação. E tem funcionado. A empresa aérea que exigir que o cliente tenha um cartão, um token ou um outro elemento de certificação está criando um complicador para o cliente. E o que ela quer é facilitar. Isso já vale até para os cartões de crédito. Já se dispensa, em muitos casos, a assinatura do titular, bastando informar o número do cartão. O cartão já dispensou a certificação – que é a nossa assinatura – para ganhar tempo.”

**Fonte: Em que casos, então, a certificação é a solução mais indicada?**

“Ela entra quando você quer ter perenidade e durabilidade na informação, para que outros possam saber que a operação foi feita. A operação ou o documento será armazenado por longo tempo, como alguns documentos públicos ou por exigência legal. Ou quando o valor da operação é tão grande que você deseja uma segurança a mais.

Enfim, a certificação não é nada mais nada menos que um processo de autenticação, não do documento, mas da autoria do documento. Em algumas operações, você tem que saber com certeza com quem está falando, quem está enviando a mensagem. Em outras, você não precisa ter certeza; você presume a certeza. A quantidade de ligações telefônicas que fazemos, e-mails e fax que transmitimos mostra que a maioria das mensagens que



trocamos dispensa um tipo de certificação mais séria. Em geral, você se contenta com o nome da pessoa no cabeçalho do e-mail, o que é facilmente falsificável.

A estrutura da ICP-Brasil funciona para uns poucos casos em que é obrigatória. Fazendo um paralelo: quando é que nós somos obrigados a ir a um cartório passar uma escritura? Em pouquíssimos casos.

Na maioria das vezes, nós fazemos os nossos negócios por documentos particulares. A ICP, da mesma forma, é obrigatória em um número limitadíssimo de casos e ela faz uma remissão para o Código Civil Brasileiro. Na maioria dos casos, a ICP não é obrigatória: você pode trabalhar com ICPs particulares, privadas e fora do sistema governamental.”

**Fonte: Com relação ao comércio eletrônico, há uma grande expectativa de aquecimento nesse tipo de transação. Essa expectativa é procedente?**

“Fala-se muito em comércio eletrônico. É um engano pensar que a certificação digital é importante para o comércio eletrônico. Na verdade, o comércio eletrônico em geral não vai usar a certificação, ou vai usar muito pouco. Na minha opinião, é muito importante para a maioria das transações comerciais justamente que não haja o processo de certificação, a fim de agilizar esse tipo de operação.”

**Fonte: Na prática, como funciona no setor público o uso da certificação digital?**

“No Governo Federal, desde 2000, as correspondências

oficiais dos ministros ao Presidente da República – propondo projetos de lei, projetos de decretos, minutas de medidas provisórias – são feitas, transmitidas e assinadas eletronicamente. Cada ministro de Estado tem seu cartão, sua senha, e os documentos são transmitidos para a Casa Civil com a garantia de autenticidade não do transmissor da mensagem, mas do autor do documento.

A certificação digital substitui a assinatura em papel. E quem recebe o documento tem a mais absoluta certeza de que foi produzido por determinado ministro, por determinada autoridade. Não se faz mais esses documentos em papel.

A Casa Civil, inclusive, recusa quando feitos em papel. Era assim nos dois últimos anos do governo Fernando Henrique, mas acho que não mudou a sistemática. Cada ministro de Estado, cada secretário de Ministério tem a sua senha, que é o seu cartão magnético, é um cartão com um chip contendo exatamente a chave privada com um algoritmo.”

**Fonte: Como será a aplicação da certificação digital em Minas?**

Será a mesma coisa: temos aqui a Advocacia Geral, a transmissão de documentos oficiais para o Palácio, a transmissão de documentos do Palácio para a Imprensa Oficial. Hoje é necessário adotar as duas formas: envia-se o documento por meio eletrônico, mas, por segurança, o papel vai atrás. Quando tivermos a certificação digital, vamos acabar com o papel. Vamos ganhar tempo.”

**Fonte: Sintetize, por favor, os benefícios da certificação digital para a administração pública.**

“Você ganha velocidade na transmissão da informação eletrônica; já tem isso, mas você passa a transmitir dados e documentos por meio eletrônico que você não poderia fazer se não estivesse na ICP-Brasil.

Não se pode, hoje, mandar um documento oficial para o governador e não assinar; eu tenho que assinar, qualquer secretário que mandar um documento oficial tem que assinar.

Não se pode, hoje, mandar um documento oficial para o governador por e-mail, ainda que o governador se disponha a receber esse e-mail.

Primeiro, o governador tem um problema de segurança: ele não sabe se quem está passando aquele e-mail é o próprio secretário ou um auxiliar dele; segundo, ele não tem certeza quanto à autenticidade do documento: ele não sabe se o documento foi modificado no meio do caminho ou se o documento não foi modificado no seu próprio computador. Com a certificação, se ele estiver assinado e alguém fizer alguma alteração, essa assinatura cai; saberemos que esse documento sofreu uma alteração.

Ganhamos na velocidade e eliminamos o office-boy em muitas circunstâncias. Ganhamos na velocidade, no tempo, na distância.”

**Fonte: Quais são as vantagens de uma entidade pública no processo de**

## **certificação digital?**

“Com a certificadora pública, você passa a ter um pouco mais de liberdade. No caso da Prodemge, por exemplo, como uma Autoridade Certificadora dentro da ICP-Brasil, passamos a ter a liberdade de, nós mesmos, emitirmos os nossos certificados, tendo as nossas autoridades de registro. Mas, provavelmente, a Prodemge não vai entrar no mercado privado para competir com empresas privadas de certificação, mesmo porque o perfil dela é voltado para servir ao Estado.

Isso equivale mais ou menos também àquela história: o Estado pode ter ou não a sua própria companhia de energia elétrica; Minas tem a Cemig. Não sei se outros estados têm, mas nem por isso o pessoal de lá está no escuro. É claro que você, tendo o serviço próprio, passa a ter uma certa liberdade. Não é bom nem ruim, depende da conveniência.”

**Fonte: Como o senhor avalia a questão da tradição do uso do documento em papel, que é algo palpável, com a entrada do documento digital, através da certificação?**

“O papel não vai acabar. Na medida em que você certifica um documento eletrônico, você passa a poder armazená-lo com segurança. Não com segurança da duração do armazenamento, mas com segurança da autenticidade do documento. Uma coisa é você achar um papel velho; outra é você achar um papel velho com uns rabiscos e uma assinatura do Beethoven embaixo. Ah, isso aqui é o original da Quinta Sinfonia!

Na medida em que o papel passou a ser assinado, ficou importante ele ser guardado. Da mesma forma, na medida em que o documento eletrônico possa ser assinado, pode-se armazenar esse documento, ele começa a ficar importante, porque ele passa a ter o valor do papel assinado. Recentemente, entreguei ao Arquivo Público Mineiro algumas dezenas de metros de papéis que eram originais de decretos desde mais ou menos 1940 até hoje. Eram os originais, que estavam guardados aqui porque são produzidos aqui. Se, mais tarde, o governador estiver fazendo assinaturas eletrônicas de decretos, eu não vou ter decretos aqui,

**“Os documentos do Qumran duraram 2 mil; estão arquivados há 2 mil anos. Não sabemos se daqui a 500 anos alguém vai ler um disquete.”**

arquivados em papel, mas arquivados eletronicamente. Ao invés de metros de papel, eu vou ter alguns centímetros de CDs numa caixinha, que eu posso, inclusive, duplicar e enviar para o arquivo até pela internet.”

**Fonte: Com relação à mídia de armazenamento dessas informações e documentos, o senhor se preocupa com os meios de recuperação das informações. Comente esse aspecto.**

“Temos que considerar as

mesmas dificuldades de um microfilme, por exemplo. Eu tenho em minha casa algumas dezenas de LPs antigos e tenho lá um toca-discos que está sem agulha. Eu estou atrás de uma agulha para esse toca-discos. Todos já estão duplicados em CD, mas eu gosto do LP. Ou seja, a minha mídia está ficando ultrapassada. Quem guardou alguma coisa naqueles disquetes de 5 ¼ e não passou para outra mídia perdeu informação. Vai ter que ir a um museu para recuperá-los – você vai ter que trabalhar com a arqueologia eletrônica. Há essas susceptibilidades. Não vamos pensar que o meio eletrônico é a grande solução. Ele tem problemas. Obviamente, na sepultura dos nossos parentes, nos cemitérios, nós vamos continuar colocando o nome na pedra, no mármore, porque nós queremos que isso dure muito. Ninguém vai largar um chip na sepultura.

A pedra é uma das mídias mais duráveis que já se descobriu. O homem da pedra descobriu, quando começou a escrever, que tratava-se de uma mídia durável. Não era só porque não tinha o papel. Não é prático, mas tem muita escrita em pedra que recuperou a nossa história. Nós não sabemos a durabilidade de um CD. A carta de Pero Vaz de Caminha já durou 500 anos; nós não sabemos se a mídia eletrônica se conserva por 500 anos. Os documentos do Qumran duraram 2 mil; estão arquivados há 2 mil anos. Não sabemos se daqui a 500 anos alguém vai ler um disquete.

A certificação permite que você passe a ter um armazenamento importante de informações, mas, eventualmente, como não é um armazenamento físico, você tem

um problema de recuperação. É mais fácil recuperar informação de um LP do que de um DVD ou de um disquete de computador, em que o armazenamento é lógico.

A certificação digital valoriza muito o armazenamento da informação eletrônica, porque ele passa a ser um armazenamento com alto grau de confiabilidade quanto à autenticidade. Ela agrega valor ao documento. Mas a certificação não acrescenta nada com relação à durabilidade. Mesmo a certificação privada, é importante, por exemplo, para documentos históricos particulares. A carta de Pero Vaz de Caminha é um documento oficial, tratava-se de um escrivão do rei na esquadra, uma autoridade pública.

De outra forma, são documentos particulares os Lusíadas, Odisseia, a Ilíada. Mesmo a certificação privada agregará valor a documentos privados arquivados com certificação digital privada.”

**Fonte: *Sistemas da Microsoft estariam adaptados para o sistema brasileiro de certificação digital. Como funciona?***


“No caso da chave pública brasileira, foi assinado, em 2002, um convênio entre o Governo brasileiro e a Microsoft. A partir daquela data, a chave pública brasileira estaria fazendo parte do sistema da Microsoft. Nós somos um dos poucos países do mundo a fazer esse acordo com a Microsoft. Como funciona: para usar o sistema de certificação, no seu computador, há o sistema de senha e contrasenha e o seu computador tem que conhecer a contrasenha da autoridade

certificadora da autoridade raiz, ou seja, essa contrasenha tem que estar nos sistemas, é a chave pública.

Se ela não estiver nos sistemas, você vai ter que baixá-la no computador. Se você vai trabalhar com a ICP, vai ter que entrar no site da autoridade raiz, baixar a chave pública no seu computador, armazenado-a na memória. Na hora em que você fizer comunicações usando assinaturas eletrônicas, o computador da outra parte, ao receber a sua mensagem, vai ter condições de lhe dizer que a autoridade raiz está garantindo a operação. Se isso não está no computador, você tem que fazer algumas operações manuais para consultar a raiz ou consultar a certificadora.

É mais ou menos isso: alguém me telefona e diz uma senha; você tem que dar a contrasenha. Aí você teria que ligar para uma terceira pessoa e confirmar se senha e contrasenha estão compatíveis, porque você não confia na ligação, mas você confia em quem vai lhe dar informações sobre a senha, que é a autoridade certificadora. Esse sistema pode ser on-line ou através de vários passos. Uma vez dentro do sistema da Microsoft, é como se houvesse uma linha com a raiz.

A Microsoft permite que, na hora que você colocar o sistema de senha e contrasenha ou de chave pública e chave privada no computador, a consulta seja feita automaticamente. E, no computador, você já pode saber se o documento é válido. Com esse acordo, isso já vem no sistema. A Microsoft só fez isso depois de ter uma declaração formal do Brasil de que a nossa Autoridade Raiz atende a uma série de requisitos

que ela solicitou. Eles quiseram auditar o sistema, mas isso nós não permitimos.” 



# ICP-Brasil

## Evolução com Equilíbrio e Correção

Evandro Oliveira

Após um tempo considerável, desde que a certificação digital no Brasil tomou rumos mais claros e específicos (a Medida Provisória 2.200-2 sobre o tema foi publicada em agosto de 2002), ainda encontramos pessoas que, mesmo atuando na área de informática, mesmo sendo profissionais qualificados, ainda não conhecem o funcionamento, aplicabilidade e exemplos práticos das vantagens de se ter a adoção de uma Infra-estrutura de Chaves Públicas (de PKI - Public Key Infrastructure).

Alguns casos de não reconhecimento chegam a repetir certa técnica muito utilizada noutro tema muito polemizado ultimamente, o software livre. Os desconhecedores utilizam da aplicação do medo, da incerteza e da dúvida (FUD, da expressão em inglês) quanto à eficácia e correção do processo de Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), com argumentos que são do domínio de parcela que nem mesmo discute o tema com qualidade.

Embora a ICP-Brasil preveja que particulares possam utilizar qualquer tipo de certificação, ainda são muitos os profissionais de informática que não entenderam em quais condições devem usar processos diferenciados de certificação digital. Entendemos que se os profissionais de TI passarem a usar certificados digitais, assinaturas eletrônicas, criptografia assimétrica e até mesmo criptografia

simétrica, com a preocupação de interoperabilidade entre estes mecanismos, constatarão que a estrutura adotada no Brasil é a mais apropriada aos propósitos de Governo e Setor Privado.

Mas como é natural que mais pessoas passem a questionar os processos existentes e vejam as vantagens do uso de certificação digital como um grande passo na melhoria e segurança dos

procedimentos e transações feitas por particulares e por estes e o poder público, o que estamos presenciando é uma crescente adoção e aceitação dos regulamentos previstos na MP 2.200-2 e nas resoluções publicadas pelo Comitê Gestor da ICP-Brasil.

Para começar a entender o funcionamento dessa estrutura, é necessário saber a diferença entre as formas e processos de certificação digital e a hierarquia adotada no País ([www.iti.gov.br](http://www.iti.gov.br)). O regulamento implantado determina que as regras devem

ser aprovadas pelo Comitê Gestor que tem representação do Poder Executivo Federal e da Sociedade Civil (com previsão de que os Poderes Legislativo e Judiciário passem a ter representação no referido Comitê). Este Comitê é assessorado por um Conselho Técnico que estuda e debate as questões técnicas, questões jurídicas e administrativas e adoção de tecnologias para promover a interoperabilidade entre certificados de autoridades certificadoras diferentes da estrutura.

**“Os desconhecedores utilizam da aplicação do medo, da incerteza e da dúvida quanto à eficácia e correção do processo de Infra-estrutura de Chaves Públicas Brasileira...”**

A Autoridade Certificadora Raiz, representada pelo Instituto Nacional de Tecnologia da Informação – ITI ([www.iti.br](http://www.iti.br)) –, autarquia vinculada à Casa Civil da Presidência da República, cuida para que a operação das autoridades certificadoras, autoridades de registro, prestadores de serviço, auditorias independentes e demais intervenientes possam atuar na estrutura com as melhores condições e funcionalidades.

As empresas da iniciativa privada e órgãos públicos já estão se posicionando de forma a escolher onde estão mais aptos e adequados a atuar com certificação digital na estrutura da ICP-Brasil e, após serem auditados para mostrar conformidade com as regras estabelecidas, recebem o credenciamento e podem atuar com os demais e servindo ao cidadão com garantias que não presenciemos em métodos de certificação não auditáveis. Cabe então a cada um desses intervenientes estudar o tema, se apresentar como capaz para desempenhar o papel que deseja e, após credenciado, se qualificar como debatedor e participe da evolução do processo.

Confiar que a estrutura estabelecida pode determinar as técnicas e tecnologias a serem adotadas e que as auditorias são realizadas com intuito de verificar o proposto e realizado pelas entidades credenciadas é mais importante do que não participar e querer que um ponto aqui e outro acolá seja modificado para atender interesses corporativos e particulares.

As regras de ICP-Brasil têm evoluído a partir da primeira estrutura montada, e devemos ressaltar

que é importantíssimo não “jogar fora” o investimento valioso já implementado e em uso no País. Não se deve nem imaginar o estrago que poderia ser feito se o Sistema de Pagamentos Brasileiro, o maior exemplo do uso prático da certificação digital no País, tivesse que ser refeito. Outro exemplo a ser referenciado daqui a alguns dias é o uso integral, por parte dos servidores da Receita Federal, de certificados digitais da ICP-Brasil.

Trabalhamos para, a cada reunião do Comitê Gestor, propor revisões que consolidem, cada vez mais, a inserção de instituições do setor público que não sejam da esfera federal, não pelo método do medo, incerteza e dúvida, mas por contribuirmos para que todos acreditem que estão fazendo a escolha por sistemas criptográficos apropriados e, a partir daí, passem a contribuir com o País na adoção e aplicação das estruturas e regras da ICP-Brasil, elevando consideravelmente os níveis de segurança nas transações que utilizem as mais variadas

tecnologias da informação.

**“As empresas privadas e órgãos públicos já estão se posicionando de forma a escolher onde estão mais aptos e adequados a atuar com certificação digital...”**

**Evandro Oliveira**

**Diretor de Auditoria, Fiscalização e Normalização  
Instituto Nacional de Tecnologia da Informação –  
ITI – Casa Civil – Presidência da República**





# Governo Eletrônico Seguro

## O projeto de segurança da informação do governo mineiro

Renata Vilhena

Com o crescente uso das novas tecnologias da informação e comunicação, principalmente com o advento da internet, e com a importância da informação enquanto recurso estratégico, a segurança da informação passou a ser uma das principais preocupações das organizações, sejam elas públicas ou privadas.

No que tange às organizações públicas, inserem-se, num contexto de modernização do Estado, propostas que envolvem novas tecnologias da informação e comunicação nas relações entre Governo e Cidadão (G2C), Governo e Empresas (G2B), Governo e Servidores (G2E) e Governo e Governo (G2G). Entretanto, nessas relações, é necessário um aparato que dê garantias e confiabilidade nas transações eletrônicas entre o Governo e a Sociedade.

Nesse sentido, o Governo do Estado de Minas Gerais, em consonância com o Programa de Governança Eletrônica, está promovendo ações com o intuito de desenvolver um projeto de implantação de Modelo de Gestão de Segurança da Informação na Administração Pública do Poder Executivo Estadual.

Sob coordenação da Secretaria de Estado de Planejamento e Gestão (Seplag) e em parceria com a Secretaria de Estado de Fazenda (SEF) e da Companhia de Tecnologia da Informação de Minas Gerais (Prodemge), o Projeto de Segurança da Informação tem como objetivo preparar as referidas instituições para alcançar um nível de segurança desejada.

Para tanto, serão realizadas atividades que vão desde uma ampla análise de riscos em seus ativos tecnológicos e seus principais processos de negócio

até a elaboração e divulgação de política de segurança da informação, capacitação de técnicos e campanhas de sensibilização de usuários, desenvolvimento de um Plano Diretor de Segurança da Informação e de um Plano de Continuidade de Negócios.

Outra ação de destaque diz respeito à capacitação tecnológica da Prodemge, que se tornará um Security Provider, contando com a parceria da Módulo, empresa brasileira com maior renome em segurança

da informação no País, com mais de 19 anos de existência e considerada uma das maiores empresas de segurança da informação do mundo. Pretende-se também obter a Certificação Internacional da Prodemge junto à BS 7799, norma de referência internacional em segurança da informação.

Enfim, esse projeto, em consonância com a Certificação Digital - projeto em andamento e coordenado pela Prodemge - proporcionará ao Governo do Estado infra-estrutura de tecnologia da informação e comunicação e processos de negócios seguros. Dessa forma, a Administração Pública do Poder

Executivo Estadual estará apta para a prestação de informações e serviços eletrônicos de forma segura, fortalecendo os mecanismos de participação dos cidadãos e transformando as relações entre Estado e Sociedade, condição fundamental para a inserção efetiva do Estado de Minas Gerais na sociedade da informação.

**“...o Governo de Minas, em consonância com o Programa de Governança Eletrônica, está promovendo ações para desenvolver um projeto de implantação de Modelo de Gestão de Segurança da Informação na Administração Pública do Poder Executivo Estadual.”**

**Renata Vilhena**

**Secretária-adjunta de Planejamento e Gestão do Governo do Estado de Minas Gerais**



# Criptografia na ficção

## Técnicas antigas e fantasias modernas

Luís Carlos Silva Eiras

A mais famosa mensagem secreta da ficção foi escrita na parede do palácio do rei Baltazar: “*Menê menê tequêl u-parsîn*”. E foi decifrada pelo profeta (e criptólogo) Daniel, conforme se lê no capítulo 5 do seu livro, e é sobre o breve futuro do rei – Baltazar morreu momentos depois da mensagem lida. Da Bíblia para cá, muitos são os exemplos de mensagens secretas em narrativas, já que boa parte da ficção conta a história de investigações e, com uma mensagem a ser decifrada, já se tem o principal da história.

É o que faz Edgar Allan Poe em *O Escaravelho de Ouro*, novela publicada em 1843. Conta como um pergaminho, descoberto numa praia, continha uma mensagem secreta e como ela foi decifrada, possibilitando que se achasse um tesouro de piratas. Allan Poe se concentra primeiro em explicar que, a partir de uma tabela de frequência, os caracteres sem sentido vão, aos poucos, revelando um texto – que, por sua vez, não faz o menor sentido! Então, Poe usa a imaginação para revelar o sentido desse texto e achar o tesouro. Uma proeza de dupla decifração.

Não era a primeira vez que Poe tocava no assunto. Em 1841, publicou num jornal que tinha recebido duas mensagens secretas de um certo W. B. Tyler, mas, apesar de ter decifrado mais de cem mensagens, estava sem tempo (!) para resolvê-las, deixando isso para os leitores. Essas mensagens

demoraram 150 anos para ser decifradas, a primeira, em 1992, por Terence Whalen, e, a segunda, em 2000, por Gil Broza, o que acabou com qualquer dúvida sobre quem era o tal W. B. Tyler. Allan Poe escreveu ainda o ensaio *Criptografia* (1842), uma prévia de *O Escaravelho de Ouro*.



Outro autor famoso que usa o assunto é Júlio Verne. Em *Matias Sandorf* (1885), a criptografia é feita através de uma tabela de três colunas de letra, sobre a qual se colocam cartões perfurados. As letras que ficam visíveis formam a mensagem. Com esse método, foi possível decifrar neste ano o manuscrito Voynich, 230 páginas de uma escrita incompreensível por mais de 5 séculos. Agora se sabe: o manuscrito não faz mesmo sentido e trata-se de uma fraude.

Mesmo em romances mais recentes, são utilizadas criptografias antigas como no *O Nome da Rosa* (1980) e *O Pêndulo de Foucault* (1988), de Umberto Eco. O primeiro usa a substituição de palavras por símbolos, o segundo, o cifrário de Vigenère, conhecido desde o século XVI.

Carl Sagan, em *Contato* (1985), é que inventa algo complicado. Imagens da transmissão de TV das

Olimpíadas de Berlim, de 1936, foram capturadas por extraterrestres e reenviadas para a Terra. Só que, no meio das frequências da velha transmissão, havia mensagens para os terráqueos. Michael Crichton, em *Esfera* (1987), é mais modesto. Uma nave espacial encontrada no fundo do Oceano Pacífico envia uma seqüência de números, que vão aos poucos sendo reagrupados até formarem mensagens inteligíveis.

Mais recente, *Cryptonomicon*, de Neal Stephenson, de 1999, faz a ligação entre os decifradores dos códigos alemães da Segunda Guerra Mundial e os hackers atuais, para quem conseguir atravessar as suas 900 páginas de idas e vindas no tempo.

No cinema, também aparecem criptografias bem variadas, que tentam, às vezes, se aproximar da realidade. Não é o caso de *Quebra de Sigilo* (1992), onde Robert Redford vai atrás de uma caixa capaz de quebrar a senha de qualquer computador, já que a caixa sabe como funcionam os números primos<sup>1</sup>. Nem de *Código para o Inferno* (1998), onde Bruce Willis se envolve com um garoto autista que sabe ler códigos secretos, que custaram um bilhão de dólares para ser desenvolvidos. Muito menos é o caso de *A Senha* (2001), onde um hacker consegue digitar mais rápido do que um programa de segurança.

Mas é o caso de *Enigma* (2001). Dougray Scott faz um matemático mais ou menos baseado em Alan Turing e mostra como os ingleses decifraram os códigos secretos dos alemães utilizando o *Colossus*, o primeiro computador. (Mostra também, numa cena de bar, Mick Jagger, o produtor do filme.) Turing é o personagem principal da peça *Breaking The Code* (1987), de Hugh Whitmore, onde conta como ele e Churchill leram todas as mensagens secretas dos

nazistas, inclusive a localização do *Bismarck*, o que possibilitou seu afundamento em 1941<sup>2</sup>.

Já o filme *U-571* exagera na importância da captura de uma máquina Enigma num submarino alemão pelos americanos. Os poloneses conheciam o funcionamento da máquina desde o início dos anos 30 e repassaram esse conhecimento para os franceses e ingleses. Eles sabiam também que não era suficiente conhecer seu funcionamento para decifrar as mensagens codificadas. Porém, a versão

em DVD tem uma boa entrevista com David Kahn, autor do clássico *The Codebreakers* (1996), ainda não editado no Brasil.

Mas é em *Uma Mente Brilhante* (2001) que essa história de decifrar códigos secretos aparece em filme da maneira mais interessante. Russel Crowe faz o matemático John Nash, que era capaz de ler códigos secretos russos escondidos em notícias de jornais e revistas. Todos imaginários.

“... boa parte da ficção conta a história de investigações e, com uma mensagem a ser decifrada, já se tem o principal da história.”

## NOTAS

<sup>1</sup> Se você também sabe como funcionam os números primos, você pode ganhar um milhão de dólares. É só responder sobre a conjectura de Riemann para o Instituto Clay de Matemática do MIT. Mais informações em <http://www.claymath.org/millennium/>.

<sup>2</sup> O funcionamento do Enigma, do Colossus e de outros métodos citados aqui pode ser testado pelo leitor em <http://www.apprendre-en-ligne.net/crypto/>.

**Luís Carlos Silva Eiras**

Analista de Sistemas da Prodemge

# Certificação Digital:

## o fio de bigode eletrônico

Confiança e segurança. As bases históricas das relações, sejam elas comerciais ou não, sobrevivem intactas, ao longo do tempo, às mudanças culturais, sociais ou tecnológicas, embora agora marcadas pela impessoalidade. São fundamentos de grandes e pequenas operações, condições para que alianças se concretizem.

O velho "fio de bigode", a caderneta do armazém ou a palavra empenhada, atributos incontesteáveis de confiança, que vêm assegurando a confiabilidade das partes envolvidas em qualquer transação comercial, ganham, como tudo na era digital, a sua versão eletrônica.

Adaptado à consolidação da internet e ao crescimento desenfreado das operações feitas através da rede mundial de computadores, um novo recurso tecnológico passa a se integrar aos poucos à vida dos brasileiros: a certificação digital, que agrega aos documentos eletrônicos, inclusive aos e-mails, a garantia de sua autoria e autenticidade, imprimindo às operações eletrônicas segurança e confiabilidade.





instantaneidade que a tecnologia imprime às comunicações passou a exigir mecanismos que assegurem às empresas, sejam elas públicas ou privadas, e às pessoas, físicas ou jurídicas, pleno aproveitamento do potencial oferecido pela tecnologia da informação.

A certificação digital é um arquivo eletrônico que acompanha um documento assinado digitalmente, contendo informações que identificam a empresa ou a pessoa com quem se está tratando na rede. Um documento eletrônico com certificação digital tem, portanto, validade jurídica. Isso garante sua autenticidade de origem e autoria, integridade de conteúdo, confidencialidade e irretratabilidade, ou seja, que a transação, depois de efetuada, não possa ser negada por nenhuma das partes.

Além da segurança e velocidade na tramitação de documentos, a certificação digital transcende a questão de espaço, ao permitir, por exemplo, que um executivo possa assinar normalmente um documento juridicamente válido a partir de qualquer ponto geográfico e em qualquer horário, com o mesmo valor de um documento em papel. Viabiliza ainda a guarda e o arquivamento seguros de documentos - oficiais ou não - com a mesma validade do seu original em papel.

O diretor de Infra-Estrutura de Chaves Públicas do ITI - Instituto Nacional de Tecnologia da Informação - autarquia federal vinculada à Secretaria da Casa Civil da Presidência da República, Renato Martini, resume os benefícios do uso dessa tecnologia. Para ele, a certificação digital agrega aos serviços maior segurança, transparência, desmaterialização, redução do consumo e trânsito de papéis, contribuindo para a diminuição do custo Brasil. Do ponto de vista institucional e social, melhora a relação do Governo com o cidadão e abre possibilidades para oferta de mais serviços pela internet - o cidadão não precisa sair de casa para ter acesso a uma série de serviços, na medida em que esteja equipado para se identificar na rede.

A assinatura eletrônica não é, no entanto, a digitalização de uma assinatura, mas um complexo sistema de códigos. Para o advogado especialista em Direito Internacional e professor gaúcho Fabiano Menke, ex-procurador



geral do Instituto Nacional de Tecnologia da Informação, a assinatura digital é um meio de agregar confiança ao ambiente virtual, confirmando a importância da autoria e identificação principalmente para questões legais. A assinatura digital agrega à internet, segundo ele, o atributo da identificação: tem, portanto, os mesmos efeitos de uma assinatura manuscrita feita no papel.

Um certificado digital contém informações relativas a seu usuário: a codificação de sua assinatura (chave privada), nome e endereço de e-mail, identificação da Autoridade Certificadora, número de série, a assinatura digital e o período de validade do certificado, que pode ser de um ou dois anos.

A chave privada do usuário pode ser armazenada em seu microcomputador, ou ainda num smart card ou token, que são mídias portáteis, que permitem seu uso a partir de outras estações. O acesso às informações contidas em seus chips é feito por meio de uma senha pessoal, determinada pelo titular. O smart card assemelha-se a um cartão magnético, sendo necessário um aparelho leitor para seu funcionamento. Já o token assemelha-se a uma chave e requer a conexão à porta USB do computador. A segurança desses três recursos é garantida também por senha.

Quanto aos preços, podem ainda ser considerados altos. Segundo o presidente da CertiSign, uma das empresas certificadoras credenciadas pela ICP/Brasil – Infra-Estrutura de Chaves Públicas, Sérgio Kulikovsky, “a média é de R\$100,00 por certificado (com validade de um ano), considerado compatível com a capacidade do usuário”. Ele prevê que esse preço caia a médio prazo: “Naturalmente, na medida em que se aumenta a demanda, o preço cai, uma vez que é estabelecido em função da quantidade”. E conclui: “Se o serviço oferecido é bom, o preço se justifica pelo benefício que ele oferece”.

### **Chaves Públicas - a questão legal**

No Brasil, a exemplo do modelo adotado pela comunidade européia, a certificação digital pode ser

concedida a pessoas físicas e a pessoas jurídicas por diferentes autoridades certificadoras que, por sua vez, podem ser públicas ou privadas. O sistema oficial brasileiro de certificação digital baseia-se na ICP-Brasil – Infra-Estrutura de Chaves Públicas Brasileira, regulamentada pela Medida Provisória 2200-2, de agosto de 2001. Ela foi instituída para “garantir a autenticidade, a integridade, a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras”. O ITI é a Autoridade Certificadora Raiz da estrutura.

De acordo com a Medida Provisória, a organização da matéria é composta por uma autoridade gestora de políticas – o Comitê Gestor da ICP-Brasil – e pela cadeia de autoridades certificadoras, composta pela Autoridade Certificadora Raiz (AC-Raiz), pelas Autoridades Certificadoras (AC) e pelas Autoridades de Registro (AR). O Comitê Gestor é composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante dos ministérios da Justiça; da Fazenda; do Desenvolvimento, Indústria e Comércio Exterior; do Planejamento, Orçamento e Gestão; da Ciência e Tecnologia; da Casa Civil da Presidência da República e do Gabinete de Segurança Institucional da Presidência da República.

O Comitê Gestor estabeleceu o padrão tecnológico mínimo para emissão da certificação digital, e os pré-requisitos para que órgãos públicos ou privados se tornem autoridades certificadoras credenciadas. O sistema dá validade jurídica a documentos enviados por e-mail e a transações feitas pela internet que estejam com certificação. Atualmente, estão cadastradas pela ICP/Brasil para atuar como autoridades certificadoras as seguintes entidades: Presidência da República, Serpro, Serasa, CertiSign, Caixa Econômica Federal e Secretaria da Receita Federal.

O advogado Fabiano Menke comenta, em artigo sobre Interoperabilidade Aplicada à ICP, “o acerto da posição adotada pelo Brasil” na aprovação da

Medida Provisória: “Sem proibir que o mercado (aqui entendido como o conjunto dos agentes não estatais) implante soluções que possam vir a ser díspares no sentido de não direcionadas à coletividade, decidiu-se por fundar uma espinha dorsal normativa comum, um tronco ou, mais precisamente, uma árvore invertida, situando no topo (na raiz da árvore invertida) uma entidade de direito público, a autarquia federal Instituto Nacional de Tecnologia da Informação - ITI, com as atribuições principais de auditar, credenciar e fiscalizar as autoridades certificadoras, autoridades de registro e prestadores de serviços de suporte que integram a ICP-Brasil”.

O advogado, que é mestre em Direito Especial – Efeitos Jurídicos da Assinatura Digital –, comenta outros benefícios de uma estrutura nacional: “Havendo uma ICP mais abrangente, como são a brasileira e a alemã, torna-se bem mais viável e atraente a celebração de acordos internacionais de reconhecimento recíproco de certificados digitais, o que possibilitará transações eletrônicas internacionais mais seguras entre empresas e entre consumidores e empresas”.

Está em tramitação no Congresso Nacional o Projeto de Lei 7316/2002, que disciplina o uso de assinaturas eletrônicas e a prestação de serviços de certificação. A necessidade e urgência de aprovação dessa Lei são defendidas pelo diretor de Infra-Estrutura de Chaves Públicas do ITI, Renato Martini: “O maior mérito é institucionalizar uma estrutura que está funcionando operacionalmente. O Brasil vai ganhar uma Lei para disciplinar a questão”, afirma. “A Lei é flexível, pode ser alterada, ao contrário da Medida Provisória; pode sofrer emendas e se adaptar à evolução da sociedade. É muito importante uma Lei disciplinando a questão da certificação digital e da estrutura de chaves públicas”, garante. O Projeto de Lei tem como relator o deputado federal Jorge Bittar.

(Confira, nesta edição, na seção “Diálogo” - página 4 - entrevista com o advogado-geral do Estado de Minas Gerais, José Bonifácio Borges de Andrada, abordando, dentre outros aspectos, a questão legal da certificação digital no País).

Pensar nos benefícios da Certificação Digital significa, em resumo, pressupor a falta de riscos no ambiente vir-

tual, uma vez que a tecnologia utilizada no processo coíbe a ação de hackers na adulteração ou interceptação de documentos ou mensagens eletrônicas. Como um documento selado, evita-se, inclusive, a leitura de conteúdos por pessoas não autorizadas.

Facilidades como essas têm ampliado de forma expressiva o seu uso: segundo Sérgio Kulikovsky, há hoje aproximadamente 200 mil certificados emitidos em todo o território nacional, a maior parte para pessoas físicas, em uso profissional. “O número de certificados tem crescido muito”, avalia. “Neste ano, registramos cerca de 50% de crescimento em relação ao ano passado.” Para o ano que vem, a expectativa é de que esse número cresça ainda mais. “A previsão é de que teremos pelo menos 1 milhão de certificados emitidos em 2005.”

Esse crescimento se justifica, para Sérgio Kulikovsky, pelos investimentos que têm sido feitos na tecnologia que viabiliza seu uso. “A tendência é um rápido crescimento daqui para a frente; o mercado necessitava de uma série de requisitos de infra-estrutura, e têm sido feitas muitas implementações, que abrem agora uma boa perspectiva.”

“A popularização da certificação digital é fundamental para garantir a privacidade e os novos direitos na sociedade em rede”, afirma o diretor-presidente do ITI, Sérgio Amadeu da Silveira. “É, também, uma forma de dar mais segurança às transações eletrônicas. Atualmente, há vários projetos para dar mais segurança aos dados que transitam na rede. Podemos citar, como exemplo, uma política de divulgação, com utilização de mídia dirigida, eventos, entre outros, com o objetivo de tornar essa tecnologia mais conhecida.”

Em sua experiência à frente da CertiSign, Kulikovsky afirma que as resistências que se anunciavam no início do processo, em grande parte atribuídas à cultura do uso do papel, aos poucos vão dando lugar à aceitação de um recurso que tem se mostrado seguro. “Havia também o desafio da tecnologia, com relação à segurança e avaliação da possibilidade de risco” – lembra. “Mas, cada vez mais, as pessoas

vêm que esse tipo de questão não procede, elas vão se convencendo de que o recurso é, de fato, bom. Que vale a pena, desde que cercado das devidas precauções.”

O leque de empresas usuárias, representantes dos mais variados setores, se abre com a consolidação da tecnologia, contemplando principalmente aqueles que envolvem públicos de relacionamento numerosos, como é o caso das empresas públicas e do sistema bancário. O Sistema de Pagamentos Brasileiro, por exemplo, que movimenta diariamente milhões de reais entre os bancos, emprega de forma efetiva a certificação digital.

Da mesma forma, a Receita Federal se prepara para tornar ainda mais segura a relação com os contribuintes: brevemente, seus 25 mil servidores estarão utilizando certificados digitais, garantindo de forma mais eficaz o sigilo fiscal. A Receita investe também na segurança da Declaração de Imposto de Renda Retido na Fonte, trabalhando em conjunto com o ITI e bancos públicos e privados no projeto de emissão dos CPFs eletrônicos - E-CPF, que deverá contemplar todos os correntistas do País, substituindo o CPF em papel pelo eletrônico a médio e longo prazos. *(Detalhes na página 32).*

Governos estaduais descobrem nessa tecnologia a solução não só para a troca de documentos entre membros do alto escalão - no envio de conteúdos formatados eletronicamente para publicação em seus diários oficiais e tramitação burocrática de projetos de Lei -, mas, também, envolvendo contribuintes, como é o caso do Governo de Pernambuco, estado brasileiro pioneiro na adoção da tecnologia.

A Secretaria da Fazenda do Estado disponibilizou um conjunto de serviços pela internet, permitindo que os contribuintes inscritos sob regime normal de apuração cumpram com suas obrigações relativas às informações econômico-fiscais, aos benefícios fiscais do Prodepe - Programa de Desenvolvimento de Pernambuco - e à escrita fiscal mensal.

Na área jurídica, que trata com grandes volumes de papel na tramitação de documentos, a adoção da



certificação digital é recebida com empenho e bons resultados. O Tribunal de Justiça do Rio Grande do Sul já adota um sistema de informatização de sessões que permite que desembargadores redijam votos em seus gabinetes, compartilhem textos e emitam acórdãos com assinatura digital para publicação em tempo real na internet. No Rio de Janeiro, o Tribunal de Justiça implementa sistema para aumentar a segurança no uso de documentos resultantes de atos notariais.

Outro exemplo de sucesso é o Peticionamento Eletrônico adotado pelo Tribunal Regional de Trabalho/ 4ª Região, no Rio Grande do Sul, que tem proporcionado, desde junho de 2004, ganhos importantes para advogados e para o sistema. Segundo o diretor da Secretaria de Informática da entidade, Eduardo Kenzi Antonini, não há ainda mensuração matemática desses resultados, devido ao curto espaço de tempo desde sua implantação, mas o ganho em segurança é evidente, e a redução de custos para advogados de todo o Estado é drástica: “Não é necessário comparecer pessoalmente para entrega das petições; a economia de tempo e dinheiro com deslocamentos e hospedagens é expressiva. É importante destacar o aspecto da segurança da informação, pois não há extravio de documentos e garante-se a autenticidade e o não-repúdio, premissas que, num Tribunal, são essenciais”.

O serviço de Peticionamento Eletrônico ganha agora proporções nacionais, com o projeto E-Doc – Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos da Justiça do Trabalho –, que está em desenvolvimento, sob coordenação do TRT 4ª Região (*Detalhes na seção Benchmarking, página 33*).

O emprego da certificação digital ganha terreno também no comércio eletrônico, garantindo segurança aos compradores virtuais de produtos em sites seguros, identificados através da imagem de um cadeado; e nas áreas médica e odontológica, em prontuários virtuais.

Sérgio Kulikovsky identifica a generalização do uso da certificação, que já extrapola as entidades detentoras de grandes públicos de relacionamento, como bancos e seguradoras. Segundo ele, o Estado é um dos grandes usuários, mas profissionais liberais também já reconhe-

cem a importância da segurança em seus relacionamentos pela internet.

Opinião semelhante tem o diretor de Infra-Estrutura de Chaves Públicas do Instituto Nacional de Tecnologia da Informação, Renato Martini. Segundo ele, o poder público, através das aplicações do Governo Eletrônico, começa a se aproximar de um sistema de certificação digital. As máquinas financeira e bancária se apresentam mais organizadas e adiantadas que os governos. “Isso não é por acaso” – explica. “Reflete a conjuntura que criou a ICP, em 2001.”

Renato Martini explica: “O sistema financeiro tradicionalmente investe em tecnologia; portanto, para o setor, isso não é novidade. Quando se trata de usar a tecnologia para implementar segurança, isso também não é novidade. Já com as aplicações do Governo Eletrônico, não é tão fácil. São instituições que trabalham com tempos diferentes”.

Para Sérgio Kulikovski, um dos aspectos mais importantes de todo o processo, no momento, refere-se às perspectivas que a construção de uma infraestrutura tecnológica satisfatória viabiliza. Ele defende a opinião de que “o principal é poder oferecer mais serviços, para mais gente, de maneira menos burocrática e mais transparente”.

As restrições impostas pela falta de segurança - característica da rede mundial de computadores - limitaram, ao longo do tempo, a oferta de serviços, que acabaram por se perpetuar no papel. Sérgio Kulikovsky defende que o foco das empresas, a partir desse momento, deve estar nas possibilidades de ampliação de seu leque de produtos e serviços com base na segurança que a certificação agrega a quaisquer operações eletrônicas.

Para ele, “o grande desafio da certificação, agora, está na criação de aplicações úteis”. Ou seja, “pensar em quem vai usar, como e por que vai usar. O foco deve, portanto, ser deslocado da tecnologia para sua aplicação inteligente e útil, abandonando mitos e focalizando o usuário”.

## **Inclusão Digital - Inclusão Social**

Se a certificação digital representa a possibilidade de oferta de um número maior de novos serviços por um universo mais abrangente de empresas, o mesmo pode ser dito da ampliação dos usuários potenciais num segmento já tão elitizado? Na opinião do diretor do ITI, Renato Martini, sim. “Atualmente, não se pode falar de inclusão social sem associar a idéia da inclusão digital”, explica. “A tecnologia está presente fortemente em todos os setores e uma das ações políticas do Governo Federal é a popularização desse serviço. Todo cidadão que tiver uma conta bancária terá acesso. Se você populariza uma tecnologia, você promove a inclusão digital. A participação do cidadão brasileiro no uso de uma tecnologia de ponta promove naturalmente a inclusão social.”

A transparência que a certificação viabiliza para usuários detentores de um certificado é considerada, pelo presidente da CertiSign, um elemento de inclusão. “O cidadão passa a ter mais acesso ao que está acontecendo, pode acompanhar e até mesmo fiscalizar os serviços que são oferecidos. Isso significa que mais gente pode ter acesso a mais informações”, afirma. Com relação à indisponibilidade de microcomputadores em domicílios de baixa renda, Kulikovsky argumenta: “Não é necessário que você tenha um computador. Com o smart card ou token (mídias portáteis), o cidadão pode ter acesso a serviços e informações a partir de qualquer lugar, de qualquer computador. Você é você em qualquer lugar onde esteja. Você deixa de ser uma senha e passa a ser você de fato; passa a ser parte do processo”.

## **Interoperabilidade**

Garantir que todos os equipamentos que compõem a infra-estrutura da certificação digital no Brasil se comuniquem, independente do modelo, fabricante ou procedência, tem sido uma preocupação das autoridades envolvidas no processo. Para o advogado Fabiano Menke, “a interoperabilidade é um atributo necessário a qualquer infra-estrutura que



pretenda atingir a coletividade”.

Na sua opinião, em artigo sobre o tema, “a idéia que influenciou a criação da ICP-Brasil foi justamente a de construir uma infra-estrutura para a coletividade, para toda a sociedade, tornando mais facilitada a comunicação entre os titulares de certificados digitais”. Ele defende a necessidade de padronização, “a fim de que, na prática, se tenha a possibilidade de assinar digitalmente, bem como verificar as assinaturas digitais a partir de qualquer equipamento”. (*Leia artigo de Fabiano Menke sobre o assunto na página 39*).

Nesse sentido, o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira aprovou, no dia 21 de outubro, através da Resolução nº 36, o regulamento para homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil. A condução do processo será feita pela Autoridade Certificadora Raiz da ICP-Brasil, o Instituto Nacional de Tecnologia da Informação - ITI, e contempla mídias como tokens criptográficos e smart cards, sistemas como de assinatura eletrônica, de autenticação de assinatura, de autoridades certificadoras e de registro, e equipamentos como os de HSM, sincronismo e carimbo de tempo, entre outros.

Segundo o diretor-presidente do ITI, Sérgio Amadeu da Silveira, “a implementação de um laboratório que checará e homologará os dispositivos de segurança, como smart cards, que suportam os certificados, é uma iniciativa relevante. Já que, a partir dessa checagem, teremos certeza, seja qual for o fabricante do dispositivo, de que ele será interoperável, ou seja, aceito em todos os sistemas. Essa iniciativa reduzirá os custos dos certificados, facilitando a sua utilização em escala. O Governo, também, tem feito um esforço de utilizar essa tecnologia como forma de reduzir o trâmite de papéis e dar rapidez aos processos”.

O estabelecimento de padrões e especificações técnicas mínimas garantirá, portanto, a sua interoperabilidade e a confiabilidade dos recursos de segurança da informação. De acordo com a Resolução, os produtos homologados terão um laudo de conformidade emitido e utilizarão o selo de homologação e seu correspondente número de identificação. Para isso, já foi inaugurado, em novembro, o primeiro Laboratório de Ensaio e Auditoria –

LEA, em São Paulo, numa parceria do ITI com o Laboratório de Sistemas Integráveis – LSI da Escola Politécnica da USP. O LEA será responsável pela homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil.

### **Chaves Públicas**

O sistema de chaves públicas prevê a certificação através de duas chaves, uma chave privada – do seu proprietário, o remetente – utilizada para assinar o documento; e uma chave pública, de conhecimento geral, que validará a assinatura, consolidadas ambas num certificado digital.

O que garante segurança ao processo é justamente a autoridade certificadora, uma terceira entidade presente no processo, que atesta para o destinatário que o remetente é quem de fato assina o documento. O processo de emissão de um certificado pressupõe o reconhecimento pessoal do interessado em ter seu certificado pela entidade certificadora. Funciona, em outras palavras, como uma assinatura reconhecida em cartório pelo tabelião, que assegura que determinada assinatura pertence de fato àquela pessoa.

A tecnologia adotada é a criptografia assimétrica. Isso quer dizer que é impossível identificar o código de uma das chaves a partir da outra. Outra característica é o fato de uma chave desempenhar exatamente função inversa à outra: uma delas – a privada – é usada para assinar o documento; a outra, a chave pública, é utilizada para reconhecer a autenticidade da assinatura.

A criptografia assimétrica se distingue da criptografia simétrica: neste caso, ambos – remetente e destinatário – conhecem o algoritmo utilizado para criptografar a mensagem, o que a torna menos segura.

As chaves garantem não só a autenticidade da assinatura, mas também a comunicação segura para troca de documentos e mensagens. Um dispositivo, o “algoritmo de hash”, é capaz de acusar qualquer

interferência na mensagem em seu trânsito entre o remetente e o destinatário.

### **Assinatura Eletrônica x Assinatura Digital**

O professor Fabiano Menke define de forma esclarecedora a diferença básica entre a assinatura eletrônica e a assinatura digital. Insere-se na primeira categoria qualquer meio para identificar o remetente de uma mensagem, como a assinatura escaneada ou digitalizada. Mesmo que a ela sejam associados outros atributos - como digitais, íris, voz - é facilmente editável, estando portanto mais sujeita a fraudes.

Já a assinatura digital é algo mais, por associar inequivocamente uma pessoa a um documento, um código exclusivo a uma pessoa. Baseia-se na criptografia assimétrica – uma parte é privada e outra é pública –, ao contrário da criptografia simétrica, em que ambas as partes compartilham um código. Pressupõe ainda uma autoridade certificadora.

### **Governo Mineiro Adota Certificação Digital**

A administração pública em Minas conta com os benefícios da tramitação de documentos e informações pela internet de forma segura, através da tecnologia de certificação digital. A Companhia de Tecnologia da Informação de Minas Gerais - Prodemge - é a Autoridade Certificadora em Minas, coordenando um dos principais projetos previstos no Programa de Governança Eletrônica do Governo do Estado.

A adoção da tecnologia no Governo de Minas foi feita dentro dos parâmetros estabelecidos pela ICP-Brasil, portanto, orientada por padrões internacionais, que colocam a administração pública mineira em condições de se relacionar virtualmente com entidades de todo o mundo.

Para emitir os certificados, a Prodemge adequou sua infra-estrutura às exigências da ICP-Brasil. Foi feito processo de licitação para contratação de uma autoridade certificadora denominada de primeiro nível

– a CertiSign foi a vencedora - que hospeda em suas instalações os utilitários e o ambiente de segurança necessários, eliminando, num primeiro momento, a necessidade de grandes investimentos para montagem da estrutura. A equipe técnica da Prodemge também desenvolveu as aplicações de suporte ao serviço.

Para o diretor do ITI, Renato Martini, a Prodemge reflete hoje a aplicação da certificação digital no serviço público: “A empresa inteligentemente escolheu um dos cenários possíveis dentro dos parâmetros do ICP, ao aproveitar uma estrutura já existente, que custou grandes investimentos ao Governo e à sociedade”. Ela poderá, como AC, cadastrar, fazer a identificação física para emissão do certificado e ter o certificado para usar em seus procedimentos dentro do Governo. “Em um outro momento, a Prodemge poderá optar por evoluir para atuar como autoridade certificadora de primeiro nível”, explica Martini. “Nesse caso, é necessária a montagem da estrutura que exige grandes investimentos, como a sala-cofre e uma estrutura complexa de criptografia. Há cenários diferentes, a regulamentação da ICP é bastante flexível, oferecendo várias possibilidades.”

A adoção da certificação digital pelo governo mineiro representa um importante passo na modernização do Estado, ao eliminar de forma substancial a necessidade da tramitação de papéis.

Os primeiros projetos de certificação digital desenvolvidos são para a Junta Comercial do Estado de Minas Gerais – Jucemg – para envio eletrônico de livros mercantis, com significativa redução da tramitação de papéis e agilização do processo. Outra aplicação é da Secretaria de Estado de Planejamento e Gestão, e abrange todo o processo de tramitação de atos normativos do Governo provenientes da Secretaria, utilizando ferramenta de workflow. A Secretaria de Governo do Estado passa a contar com o Sistema Integrado de Processamento de Atos - SIPA -, destinado aos atos de provimento de cargos comissionados. A assinatura digital para responsáveis por esses atos representa também mais agilidade e economia na tramitação de papéis.

Outras aplicações que se beneficiarão de forma efetiva do serviço são a tramitação de informações e documen-



tos da Secretaria da Fazenda com os contribuintes do ICMS; a gestão eletrônica de documentos da Junta Comercial, que representa grandes volumes de papel; o relacionamento da Secretaria de Planejamento e Gestão com os fornecedores de serviços e produtos para o Estado; o envio de documentos oficiais para publicação pela Imprensa Oficial do Estado e a identificação segura de usuários dos sistemas corporativos do Estado, entre várias outras.

## **Empresas públicas estaduais e a certificação digital**

O Instituto Nacional de Tecnologia da Informação - ITI vem trabalhando com as empresas da ABEP – Associação Brasileira de Empresas Estaduais de Processamento de Dados-, a fim de consolidar a tecnologia junto aos governos estaduais. Segundo o diretor do Instituto, Renato Martini, já foram promovidos encontros em Brasília, com o presidente do Conselho da entidade, Marcos Vinícius Ferreira Mazoni, e com os presidentes das empresas estaduais de processamento de dados em Florianópolis, na última edição do Secop – Seminário Nacional de Informática Pública.

O ITI conduz um projeto de comunicação que visa a esclarecer o tema para as áreas públicas estadual e municipal. “Entendemos que a entrada da certificação digital para o serviço público é através das empresas estaduais de informática e chamamos a Abep para ser protagonista nesse processo, através de uma ação coordenada que contribua para a institucionalização do projeto.” Martini argumenta que é importante que as empresas públicas se organizem para ter um padrão, se coordenem e desenvolvam um projeto coletivo.

Para ele, trata-se de uma tecnologia complexa. “Daí a importância de explicar ao gestor público o seu funcionamento e benefícios. Estamos fazendo contato com os profissionais da área pública. Pernambuco tem hoje seus procedimentos fazendários baseados na certificação digital. Foi o Estado que saiu na frente. Há também boas iniciativas no Poder Judiciário. Mas é possível perceber um

desnível no conhecimento e aplicação da certificação digital entre os estados – alguns muito avançados, outros, não.”

O projeto do ITI busca justamente levar ao gestor público esse conhecimento. “Estamos elaborando guias, manuais, com conteúdo esclarecedor e texto de fácil entendimento.” O material será produzido pela Universidade Federal de Santa Catarina, que tem convênio com o ITI.

## **Dicas do ITI para maior segurança na utilização da certificação digital**

(fonte: site do ITI)

Primeiramente, deve-se lembrar que o certificado digital representa a “identidade” da pessoa no mundo virtual. Assim, é necessária a adoção de alguns cuidados para se evitar que outra pessoa possa praticar negócios jurídicos, acessar páginas na internet e realizar transações bancárias em nome do titular do certificado. Recomendações para o uso de um certificado digital:

- a senha de acesso da chave privada e a própria chave privada não devem ser compartilhadas com ninguém;
- caso o computador onde foi gerado o par de chaves criptográficas seja compartilhado com diversos usuários, não é recomendável o armazenamento da chave privada no disco rígido, pois todos os usuários terão acesso a ela, sendo melhor o armazenamento em disquete, smart card ou token;
- caso a chave privada esteja armazenada no disco rígido de algum computador, deve-se protegê-lo de acesso não-autorizado, mantendo-o fisicamente seguro. Nunca deixe a sala aberta quando for necessário sair e deixar o computador ligado. Utilize também um protetor de tela com senha. Cuidado com os vírus de computador, eles podem danificar sua chave privada;
- caso o software de geração do par de chaves permita optar entre ter ou não uma senha para prote-

ger a chave privada, recomenda-se a escolha pelo acesso por meio de senha. Não usar uma senha significa que qualquer pessoa que tiver acesso ao computador poderá se passar pelo titular da chave privada, assinando contratos e movimentando contas bancárias. Em geral, é bem mais fácil usar uma senha do que proteger um computador fisicamente;

- utilize uma senha longa, com várias palavras, uma vez que existem programas com a função de desvendar senhas. Deve-se evitar o uso de dados pessoais como nome de cônjuge ou de filhos, datas de aniversários, endereços, telefones ou outros elementos relacionados com a própria pessoa. A senha nunca deve ser anotada, sendo recomendável sua memorização.

## Como verificar uma assinatura digital?

Fonte: site da CertiSign

**Antes de confiar no conteúdo de um e-mail assinado digitalmente, você precisa verificar se o certificado utilizado para assiná-lo é legítimo. Nesse caso, a assinatura é verdadeira e você pode confiar no conteúdo da mensagem que recebeu, pois ela realmente foi enviada pela pessoa ou empresa que a está assinando.**

**Não ter esse cuidado pode significar confiar numa mensagem falsa, fraudada, em nome da pessoa ou empresa que a está assinando. Por isso, é importante verificar sempre a validade da assinatura digital antes de confiar nos e-mails e newsletters que você recebe.**

**Certificado válido significa assinatura verdadeira.**

**O procedimento de verificação é diferente para cada programa de e-mail.**



## Webmail

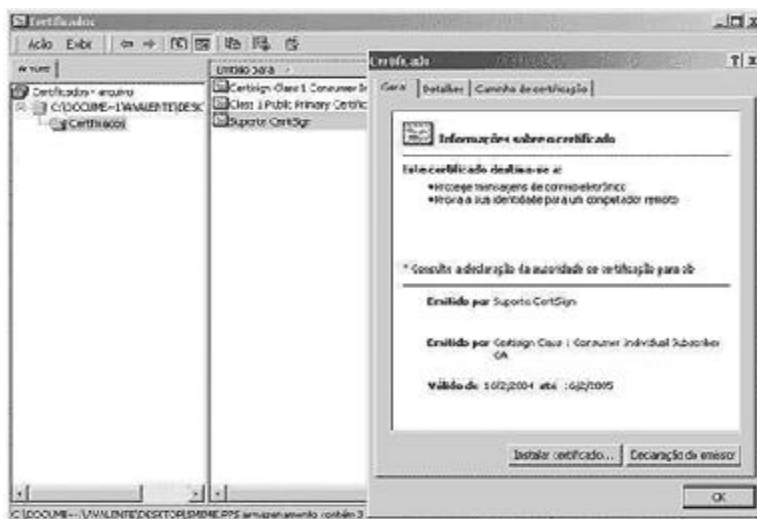
Quando recebemos um e-mail assinado digitalmente através de um webmail, o mesmo entende que a assinatura digital é um mero arquivo anexo (Smime.p7s) conforme a imagem abaixo:



Para poder verificar essa assinatura, você pode clicar no arquivo anexo e salvar o mesmo em sua área de trabalho.

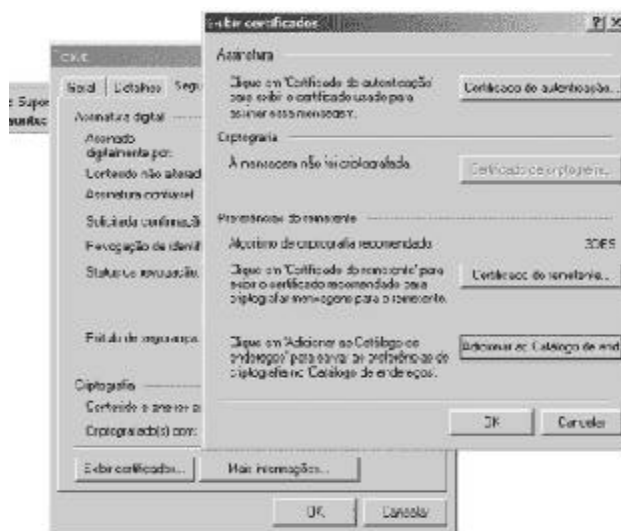
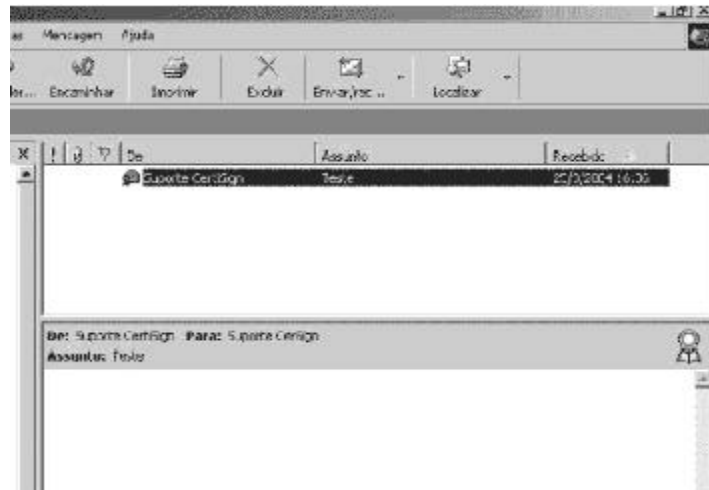


Após ter salvo o arquivo, você poderá dar um duplo clique no mesmo e verificar a assinatura digital que foi utilizada para assinar o e-mail que lhe foi enviado.



## Outlook

Ao receber um e-mail assinado, você irá visualizar uma chancela em vermelho no e-mail recebido.



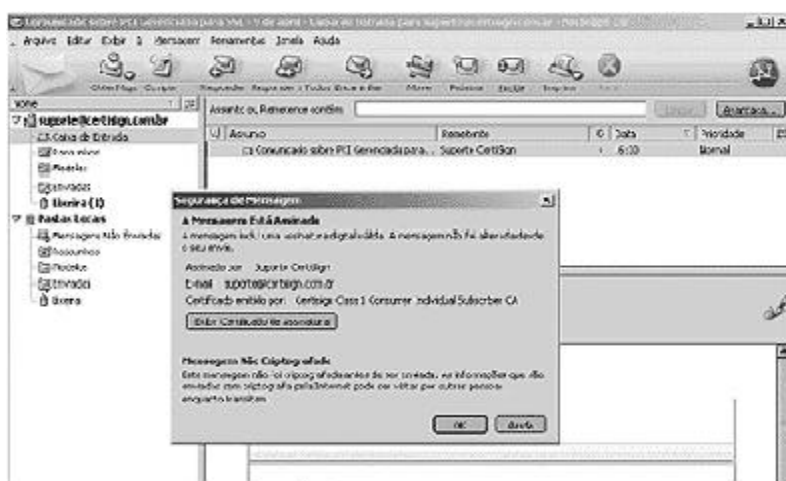
Para verificar a assinatura do emissor, você deve clicar na mesma e, em seguida, nas opções "Exibir certificados" - "Certificado de autenticação".

Em seguida, lhe será mostrado o certificado digital que foi utilizado para assinar a mensagem.



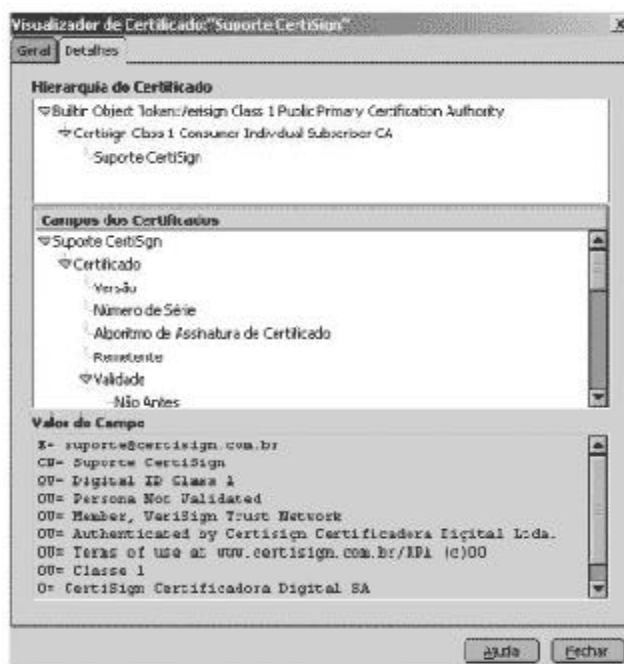
## Netscape

Ao receber um e-mail assinado utilizando o NetScape, você poderá visualizar uma “caneta” no cabeçalho da mensagem, representando que a mesma foi assinada digitalmente.



Para que você possa verificar a assinatura digital contida na mensagem, você deve clicar duas vezes neste ícone “Caneta” que a mesma irá lhe mostrar os dados referentes à certificação digital.

Para que você consiga todas as informações referentes a este certificado, você deverá clicar em “Exibir Certificado de Assinatura”.



## Glossário

**Autenticidade:** garantia de que a mensagem foi enviada por um remetente determinado e de que não é possível que outra pessoa se passe por ele.

**Autoridade Certificadora:** entidade autorizada a emitir certificados que vinculem uma determinada chave pública ao seu titular. Tem ainda outras atribuições, entre elas suspender, renovar ou revogar certificados digitais e emitir listas de certificados revogados.

**Confidencialidade:** atributo da mensagem protegida que garante que, após enviada, só será lida pelo destinatário e mais ninguém.

**Criptografia:** ramo das ciências exatas que tem como objetivo escrever em cifras. Trata-se de um conjunto de operações matemáticas que transformam um conteúdo em um texto cifrado.

**Garantia de Autoria:** presunção de que a mensagem é de fato assinada pela pessoa que se identifica.

**Interoperabilidade:** é pressuposto de uma infra-estrutura e pode ser definida como a capacidade que possuem os aparelhos e equipamentos que dela fazem parte de comunicarem-se entre si, independentemente de sua procedência ou de seu fabricante. (Fabiano Menke)

**Integridade:** garantia de que a mensagem que chega ao destinatário é exatamente a mesma que saiu do remetente, não tendo sofrido qualquer alteração em nenhuma de suas partes.

**Não-repúdio:** garantia de que o titular do certificado e autor da mensagem não pode negar a autoria de determinado documento. Numa situação assim, será dele o ônus de comprovar que seu certificado foi utilizado indevidamente.

**PKI:** tradução da expressão inglesa Public-Key Infrastructure - Infra-Estrutura de Chaves Públicas

**Token e smart card:** são hardwares portáteis que funcionam como mídias armazenadoras. Em seus chips, são armazenadas as chaves privadas dos usuários.

### Saiba Mais

---

Instituto Nacional de Tecnologia da Informação  
[www.iti.br](http://www.iti.br)

---

Infra-Estrutura de Chaves Públicas  
[www.icpbrasil.org](http://www.icpbrasil.org)

---

Companhia de Tecnologia da Informação do Estado de Minas Gerais  
[www.prodemge.mg.gov.br](http://www.prodemge.mg.gov.br)

---

CertiSign  
[www.certisign.com.br](http://www.certisign.com.br)

---

Tribunal Regional do Trabalho 4ª Região  
[www.trt4.gov.br](http://www.trt4.gov.br)

---

Módulo Security  
[www.modulo.com.br](http://www.modulo.com.br)



**Embora ainda em fase de consolidação no País, o uso da certificação digital ganha espaço em importantes setores da prestação de serviços públicos.**

**A seção Benchmarking mostra dois exemplos de projetos abrangentes e suas perspectivas para um número considerável de cidadãos brasileiros.**

## Receita Federal



Os 25 mil funcionários da Receita Federal, em todo o País, já se integram à crescente parcela de usuários da certificação digital. O órgão investe ainda na adoção dessa tecnologia para os contribuintes, ampliando o leque de serviços oferecidos pela internet, através do e-CPF ou CPF eletrônico, certificados digitais emitidos com a chancela do ICP-Brasil e que viabilizarão outro importante projeto: o Serviço Interativo de Atendimento Virtual, através do qual o contribuinte terá acesso, pelo computador, a serviços prestados atualmente apenas de forma presencial.

O projeto é conduzido em parceria com o ITI e bancos públicos e privados, para emissão de CPFs eletrônicos, que substituirão, a médio e longo prazos, o CPF em papel. As instituições bancárias deverão emitir um smart card contendo o certificado digital do cliente, com chancela da ICP-Brasil e o número de CPF do correntista. Esse talvez seja o mais

abrangente projeto em andamento no País, considerando-se o número de correntistas de bancos e a capilaridade das instituições bancárias.

Segundo o chefe da Divisão de Segurança da Informação da Receita Federal, Ariosto de Souza Júnior, a adoção da tecnologia para os funcionários e para os públicos de relacionamento da instituição se deve principalmente à consolidação da internet como canal de comunicação com o contribuinte: "Grande parte das informações com as quais lidamos são protegidas por sigilo fiscal, o que torna restrito o atendimento que podemos prestar se não tivermos a certeza de que o autor da demanda é efetivamente o contribuinte", explica.

Para ele, a certificação digital trará maior comodidade ao contribuinte, agilizará o atendimento aos processos e agregará maior segurança, consolidando, por

exemplo, um dos serviços importantes da Receita que é a entrega das declarações do Imposto de Renda: "Sem adotarmos a certificação digital, podemos receber as declarações via internet, mas alguns problemas que poderiam ser resolvidos remotamente acabam demandando o atendimento presencial, gerando desnecessárias filas nas delegacias da Receita".

Ele explica ainda como a tecnologia agregará agilidade ao processo: "Se recebemos um número cada vez maior de declarações via internet, a tendência é a Receita começar a dar encaminhamento aos processos todos de forma digital. Assim, por exemplo, quando um fiscal for analisar um processo, ele poderá assiná-lo eletronicamente com o seu e-CPF e aquele ato terá validade jurídica. A medida traz segurança aos sistemas informatizados da instituição e mais conforto também aos funcionários que, pelos métodos

tradicionais, têm que lembrar várias senhas para acesso a diferentes sistemas da Receita.

Ariosto de Souza Júnior lembra o processo de utilização da internet para oferta de produtos da Receita, que teve início em 1996, quando foram disponibilizadas somente a legislação tributária, informações de comércio exterior e trocas de informações com o contribuinte via correio eletrônico: “Em 97, a Receita disponibilizou o Recetanet, que é usado por 96% dos contribuintes brasileiros. Em 2004, o site da Receita registrou um total de 130 milhões de acessos e a entrega de 32 milhões de declarações. O serviço, que antes era utilizado apenas para a entrega das decla-

rações, já ampliou o atendimento a mais 120 outros documentos. Começamos então a disponibilizar serviços de consulta a aplicações, como a consulta à irregularidade fiscal e certidão negativa. Posteriormente, desenvolvemos aplicações para envio de dados como a declaração de isento, entre outras”.

A adesão dos usuários impôs, segundo Souza, a necessidade da implantação de novos recursos: “Avançamos até o limiar do que poderia ser oferecido sem ferir o sigilo fiscal. Como grande parte dos dados armazenados na Receita são protegidos por sigilo fiscal, chegamos no limite do que poderíamos fornecer sem a identificação do contribuinte”.

O processo de implantação da certificação digital passou pela aquisição de 27.500 smart cards, em fevereiro deste ano. Foram montados dois laboratórios de testes – um em Belo Horizonte, outro em Brasília –, além de um projeto piloto na Delegacia da Receita Federal em Contagem (MG). O projeto abrange 567 unidades da Receita Federal em todo o País.

“Usamos todo esse arranjo” – explica Ariosto Souza – “porque a Receita não quer aumentar o volume de atendimentos de balcão. Todo esse processo é para reduzir o atendimento presencial e facilitar a relação do contribuinte com a Receita”.



## **Tribunal Regional do Trabalho 4ª Região** **RIO GRANDE DO SUL**

No Rio Grande do Sul, o Tribunal Regional do Trabalho – 4ª Região implementou o primeiro sistema de Peticionamento Eletrônico do País, com adoção da certificação digital.

O serviço permite o envio eletrônico de petições através da internet, sem a necessidade da apresentação posterior dos ori-

ginais. A segurança da transação é garantida pela assinatura digital com utilização de certificados emitidos pela ICP-Brasil, que possuem validade jurídica de acordo com a Medida Provisória 2200-2.

Segundo o diretor da Secretaria de Informática do TRT, Eduardo

Kenzi Antonini, o projeto piloto foi desenvolvido com 20 advogados em dezembro de 2003 e, já em maio de 2004, o serviço foi ampliado para todos os interessados. Nos primeiros cinco meses do Peticionamento Eletrônico, cerca de 200 dos 8 mil advogados cadastrados no TRT4 já haviam adotado essa forma de trabalho.

Embora o pequeno tempo de uso do serviço não permita ainda medir com exatidão os seus resultados, o ganho em segurança e a redução de custos para advogados de todo o Estado é evidente. As vantagens se estendem também ao jurisdicionado, que ganha em rapidez e segurança; e ao sistema do judiciário, que ficou mais seguro - não há extravio de documentos -, ágil e simples. A autenticidade e o não-repúdio são, afinal, premissas essenciais num Tribunal.

### **Como funciona**

O TRT4 permite o envio de petições ao Tribunal e a todas as Varas do Trabalho da 4ª Região. Não estão contempladas no serviço as petições iniciais de 1ª instância e/ou seus aditamentos.

Em primeiro lugar, o usuário deve adquirir um certificado digital de qualquer entidade credenciada à ICP-Brasil. Para efetivar seu cadastro, é só acessar um formulário na internet e preencher os dados requisitados. No site do Tribunal, é possível fazer o download do Assinador Eletrônico; uma vez instalado no computador do usuário, o programa deverá ser usado para assinar eletronicamente suas petições, antes de enviá-las ao TRT.

Os arquivos são criptografados durante o envio. Ao receber a petição enviada eletronicamente,

o Tribunal analisa o arquivo recebido, verificando a validade da assinatura digital e se ela pertence efetivamente à petição enviada; consulta a data e a hora do recebimento junto ao Observatório Nacional; e gera um recibo da petição, que poderá ser impresso ou armazenado pelo advogado.

### **Projeto E-Doc**

O serviço de Peticionamento Eletrônico ganha agora proporções nacionais, com o projeto E-Doc – Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos da Justiça do Trabalho –, que está em desenvolvimento, a cargo do Grupo de Planejamento da Informatização da Justiça do Trabalho, coordenado pelo TRT da 4ª Região.

O objetivo é disponibilizar, através de infra-estrutura distribuída nos tribunais que compõem a Justiça do Trabalho, um sistema de envio e recebimento eletrônico de documentos aos Tribunais Regionais e ao Tribunal Superior do Trabalho. Da mesma forma que o Peticionamento Eletrônico do TRT4, será exigido o uso de certificados digitais emitidos pela ICP-Brasil, garantindo validade jurídica ao serviço.

Quando implantado, o E-Doc agregará ao sistema da Justiça do Trabalho mais agilidade e desburocratização, redução de custos e integração dos tribunais.

## Certificação Digital: o fim dos Cartórios?

**José Eisenberg**



A certificação digital – a atribuição de valor jurídico, através de criptografias personalizadas, para assinaturas enviadas através da rede mundial de computadores – apresenta um desafio instigante para o futuro da burocracia pública e privada, tal qual ela se conformou ao longo da história do Brasil. O nosso sistema jurídico, herdeiro do sistema centralizado português e sua estrutura oligárquica de

certificação de assinaturas em papel, em particular no Direito Civil, distribui a autoridade pública de certificação no mundo privado através de um sistema de cartórios, funcional e geograficamente atribuído, onde ainda funcionam antigas instituições de parentesco na reprodução do exercício daquela autoridade.

Para a economia, os cartórios representam simultaneamente custos de transação, a serem devidamente incluídos na formação de preços, e segurança para essas mesmas transações, em caso de litígios. Para o Direito, eles são entidades privadas investidas de autoridade pública cuja certificação confere validade a um documento envolvendo uma ou mais partes de um processo. Já para os cidadãos, os cartórios em geral representam uma senha para uma nova fila, uma taxa que subiu de novo, uma cópia autenticada da identidade que não ficou boa, ou, no caso dos mais afortunados, finalmente a escritura lavrada de uma casa própria.

A certificação digital, no modelo regulamentado pela ICP-Brasil (Infra-Estrutura de Chaves Públicas) na Medida Provisória 2200-2 de 8/2001, criou uma estrutura hierárquica de autoridades certificadoras, centralizadas em uma autoridade certificadora raiz

e regulada por uma nova agência, o Comitê Gestor da ICP-Brasil. As autoridades certificadoras, bem como as autoridades de registro abaixo delas, formarão um mercado que será regulado por esta agência, sendo cada ente auditado, credenciado e fiscalizado por uma entidade de direito público, o Instituto Nacional de Tecnologias de Informação (ITI), a autoridade certificadora raiz. Hoje ainda testemunhamos os

primeiros passos no sentido da implementação desse sistema, já que são em torno de seis autoridades certificadoras, sendo a maioria órgãos vinculados à União.

Para a economia, a certificação digital representa uma potencial diminuição dos custos de transação que resultam das prerrogativas de certificação dos cartórios. Amplia-se um mercado de certificação de documentos, mais moderno tecnologicamente e mais ágil do ponto de vista do tempo de transação, que certamente fará com que pessoas jurídicas, com cada vez mais frequência, incorram nos custos iniciais de investimento em uma estrutura de certificação digital (seja um *token*, um *smart card* ou uma chave no PC) para poder agilizar e diminuir os custos dessas transações. Em transações internacionais, em particular, ter acesso à certificação digital já está se tornando um imperativo.

Quanto à segurança das transações econômicas, ela será indubitavelmente maior. Uma criptografia assimétrica não é mais manipulável e/ou perigosa do que um carimbo, um selo ou uma rubrica de escrivão de cartório. Há certos mitos sobre as novas tecnologias de informação e comunicação que precisam ser abertamente combatidos e este é um deles.



Computadores são uma das formas mais seguras de armazenamento de informação já concebidas pela humanidade.

Já para o Direito, a certificação digital pode possibilitar uma verdadeira revolução no sistema processual. Com o grau de segurança e sigilo que a internet hoje permite, a certificação digital pode contribuir de forma decisiva para que os tribunais brasileiros esvaziem suas estantes e arquivos de processos. Desde acórdãos com assinatura digital publicados on-line, até a tramitação interna mais cotidiana de processos e seus documentos, a assinatura digital pode ser um instrumento vital que faltava ao Direito brasileiro para que ele, finalmente, converta sua rica estrutura de processamento de litígios e de garantia de direitos em uma ágil rede de interações capaz de mobilizar a capilaridade social de nossos tribunais em práticas democráticas de acesso à justiça para os menos favorecidos.

O sistema processual brasileiro certamente tem suas deficiências institucionais. Entretanto, a sua falta de celeridade resulta primordialmente de um aparato burocrático pouco preparado para acomodar as demandas advindas da sociedade, bem como a energia investigativa de um Ministério Público ativo e independente. Ainda que a informatização não tenha atingido a vasta malha de tribunais de justiça no Brasil, qualquer medida que leve o Estado a fazer os investimentos necessários para tornar o judiciário mais ágil deve ser louvada. Particularmente, se ela aumenta, simultaneamente, o grau de transparência das suas atividades.

Para os cidadãos, no curto prazo, tudo que diz respeito à certificação digital não passa de conversa de gente que mexe com computador. No longo prazo, porém, a inclusão digital é um problema educacional estrutural da sociedade brasileira que precisa ser atacado com políticas públicas dirigidas, porém universais, para que as novas gerações de brasileiros estejam devidamente equipadas com os instrumentos necessários ao pleno exercício da cidadania. A certificação digital é somente mais um prenúncio da premência desta outra agenda já que, caso ela se

consolide e encontre tanto no mercado quanto no poder público a receptividade e atenção que merece, não demorará muito para que nós passemos a ser uma sociedade dividida entre os com-CPF e os sem-CPF, mas também entre os que têm ou não assinatura digital. Seria ela o Registro Geral (R.G.) do futuro?

A grande virtude da Certificação Digital reside na possibilidade da descartorialização do nosso sistema de autenticação e certificação de transações entre entidades de direito civil, sejam elas pessoas físicas ou pessoas jurídicas. Abrir um mercado sem cartórios não é uma garantia contra a sua oligopolização (nem uma idéia tão inovadora assim nos tempos de hoje), mas faz sentido. Faz mais sentido ainda a centralização mantida na estrutura de autoridades constante na medida provisória aprovada sobre o assunto. Haverá sempre um problema de regulação desse mercado, e os agentes públicos e da sociedade civil precisam efetivamente operar nos diversos níveis da burocracia regulatória para agir como efetivos fiscalizadores da qualidade dos serviços de certificação digital oferecidos.

A segurança do sistema virá. Mas pairam dúvidas. Curiosamente, no dia 1º de novembro, a página do ITI para divulgação de seu 2º Fórum de Certificação Digital estava fora do ar, tendo sido invadida por um protesto que clamava "*Nós somos os fora-da-lei de uma lei que não existe*".

Todos, pelo jeito, até mesmo os invasores da página do ITI, aguardam a aprovação do Projeto de Lei 7316/2002, que disciplinará o uso de assinaturas eletrônicas e o mercado de certificação digital. Eu, de minha, parte, espero que, no longo prazo, possamos olhar para os passos que damos hoje como o começo do fim de uma era dos cartórios no Brasil.

**José Eisenberg** - Professor de Ciência Política (IUPERJ), é co-organizador de *Internet e Política: teoria e prática da democracia eletrônica* (Belo Horizonte: Ed. UFMG, 2001) e autor de vários artigos sobre novas tecnologias de informação e comunicação.

# Fonte

A Tecnologia da  
Informação na  
Gestão Pública

Dezembro de 2004

**Contribuições acadêmicas  
exclusivas, focadas nos  
temas certificação digital e  
segurança da informação**



UNIVERSIDADE  

---

CORPORATIVA  

---

P R O D E M G E



# Considerações sobre a interoperabilidade aplicada à infra-estrutura de chaves públicas



## Fabiano Menke

Advogado. Ex-procurador-geral do Instituto Nacional de Tecnologia da Informação. Membro da Comissão Técnica Executiva da Infra-Estrutura de Chaves Públicas Brasileira. Mestre em Direito pelo Curso de Pós-Graduação de Concentração em Direitos Especiais. Professor de Direito Civil no Centro Universitário Ritter dos Reis, Canoas, RS.

## RESUMO

O artigo analisa a interoperabilidade aplicada à Infra-Estrutura de Chaves Públicas (ICP). Principia delineando noção geral de interoperabilidade e, após, versa especificamente sobre a interoperabilidade existente numa ICP. Explica o significado da palavra “infra-Estrutura”, que é de fundamental importância para a análise do objeto de estudo. A abordagem é feita com ênfase na Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), instituída pela Medida Provisória nº 2.200. Além disso, apresenta a interoperabilidade como gênero que se divide em dois, a interoperabilidade formal, operacional, técnica ou objetiva, e a interoperabilidade substancial ou subjetiva.

*Palavras-chave:* interoperabilidade; infra-estrutura (de chaves públicas).

### 1. Noção geral de interoperabilidade

Uma noção geral de interoperabilidade pode ser obtida a partir de um exemplo prático, como o regulado pela Diretiva da Comunidade Européia nº 96/48, de 23 de julho de 1996, que trata da “interoperabilidade do sistema ferroviário transeuropeu de alta velocidade”. Nos considerandos dessa Diretiva, é dito: “para que os cidadãos da União, os operadores econômicos e as

coletividades regionais e locais se beneficiem plenamente das vantagens decorrentes da criação de um espaço sem fronteiras, importa, designadamente, incentivar a interconexão e a interoperabilidade das redes nacionais de trens de alta velocidade, bem como o acesso a essas redes”. Observe-se bem, a Comunidade Européia resolveu adotar uma diretiva estabelecendo critérios e padrões comuns para possibilitar que um trem francês possa sair de Paris, passar por cidades alemãs

e finalmente chegar a Viena, na Áustria, sem que no percurso encontre qualquer problema de incompatibilidade. Para atingir esse objetivo, foram criadas as ETI, que são as especificações técnicas de interoperabilidade, “a que cada subsistema é objeto a fim de satisfazer os requisitos essenciais, estabelecendo as necessárias relações funcionais recíprocas entre os subsistemas do sistema ferroviário transeuropeu de alta velocidade”.

Talvez esse exemplo seja o mais elucidativo para ilustrar o que seja, numa acepção mais geral, interoperabilidade. Por meio dele, verifica-se que a interoperabilidade é um apanágio necessário de qualquer infra-estrutura e pode ser definida como a capacidade que possuem os aparelhos ou equipamentos que dela fazem parte de comunicarem-se entre si, independentemente de sua procedência ou do seu fabricante. Num sistema de telefonia celular, por exemplo, a interoperabilidade permite que dois indivíduos que tenham aparelhos diversos e linhas telefônicas de operadoras diversas possam conversar sem problemas. O mesmo princípio se aplica a uma infra-estrutura de chaves públicas, ou seja, “A” poderá se comunicar eletronicamente com “B”, ainda que os seus certificados digitais e os equipamentos que utilizem para criar e verificar assinaturas digitais não

sejam fornecidos pelo mesmo fornecedor (aqui incluídos a respectiva autoridade certificadora emissora do certificado digital e os fornecedores de *hardware* e *software* utilizados para criar e verificar assinaturas).

## 2. Infra-Estrutura e ICP-Brasil

Não raro, os debates sobre os temas atinentes às assinaturas e certificados digitais fecham os olhos para uma característica fundamental de uma infra-estrutura de chaves públicas (ICP), qual seja, a de que, antes de tudo, e por mais pleonástico e óbvio que possa soar, uma ICP é uma infra-estrutura<sup>1</sup>. E por ser uma infra-estrutura é que a interoperabilidade lhe é ínsita. Portanto, seja qual for a infra-estrutura (de energia elétrica, de saneamento básico, de ferrovias, de telefonia fixa, de telefonia móvel, de chaves públicas, etc.), a palavra interoperabilidade, no mais das vezes, estará presente e dela será um atributo indispensável, sempre que o serviço fornecido tiver por escopo atingir a coletividade.

Insistindo no ponto, uma infra-estrutura de chaves públicas tem o mesmo princípio de qualquer outra instalação estrutural posta à disposição da sociedade, qual seja o de prover um serviço que pode ser obtido por qualquer interessado. Como é sabido, o termo infra-estrutura de chaves públicas é tradução da expressão da língua inglesa: *public-key infrastructure (PKI)*. Os norte-americanos bem souberam esclarecê-la, partindo, primeiramente, da própria definição da palavra infra-estrutura. **Carlisle Adams** e **Steve Lloyd**, na obra *Understanding Public-Key Infrastructure*<sup>2</sup> enfatizaram que uma infra-estrutura se caracteriza por

ser uma *pervasive substrate*, ou seja, uma fundação que dissemine algo para um amplo ambiente ou para um grande universo de interessados. Salientam que duas infra-estruturas comuns são a de comunicações eletrônicas e a de energia elétrica. Asseveram que o princípio de ambas é idêntico: a infra-estrutura existe para que qualquer usuário possa simplesmente acoplar-se a ela e dela fazer uso quando necessário.

A infra-estrutura uniforme evita que sejam aplicadas soluções díspares por cada entidade.

Quanto a esse ponto, é elucidativa a explicação de **Adams** e **Lloyd**: *"The pervasive security infrastructure is fundamentally the sensible architecture for many environments. This architecture avoids piecemeal, point-to-point, ad hoc, non-interoperable solutions, thereby introducing the possibility of manageable, consistent security across multiple applications and computing platforms. It is not difficult to imagine the chaos that would result from every pair of communicants running their own communications lines, or from every person running his/her own power generator at his/her own arbitrarily chosen voltage and current. Many facets of both ancient and modern society demonstrate that the uniformity and convenience offered by a well-designed, well-defined, pervasive infrastructure is worth the effort involved in the design and definition stages"*<sup>3</sup>.

Atente-se bem à observação contida no texto citado: uma infra-estrutura de segurança disseminada, uniforme, evita soluções díspares, isoladas, não interoperáveis. O exemplo fornecido do

caos que resultaria do fato de cada indivíduo operar as suas próprias linhas de comunicação ou de geração de energia é emblemático.

Daí, no meu entender, o acerto da posição adotada pelo Brasil no que toca ao modelo de infra-estrutura de chaves públicas escolhido por meio da Medida Provisória nº 2.200 e regulações posteriores. Sem proibir que o mercado (aqui entendido como o conjunto dos agentes não estatais) implante soluções<sup>4</sup> que podem vir a ser díspares no sentido de não direcionadas à coletividade, decidiu-se por fundar uma espinha dorsal normativa comum, um tronco ou, mais precisamente, uma árvore invertida (*inverted tree*)<sup>5</sup>, situando no topo (na raiz da árvore invertida) uma entidade de direito público, a autarquia federal Instituto Nacional de Tecnologia da Informação – ITI, com as atribuições principais de auditar, credenciar e fiscalizar as autoridades certificadoras, autoridades de registro e prestadores de serviços de suporte que integram a ICP-Brasil.

O modelo adotado pelo Brasil é idêntico ao alemão<sup>6</sup>. Lá, uma divisão do órgão regulador *Regulierungsbehörde für Telekommunikation und Post (Reg-TP)*, com natureza de direito público e vinculada ao Ministério da Economia e Tecnologia, desempenha o mesmo papel que o Instituto Nacional de Tecnologia da Informação, ou seja, credencia, fiscaliza e emite certificados digitais para os prestadores de serviços de certificação (*Zertifizierungsdiensteanbieter*) do primeiro nível hierárquico da cadeia. Até o presente momento, vinte e três *Zertifizierungsdiensteanbieter* já obtiveram credenciamento pe-



rante a RegTP. Entre os credenciados, encontram-se os correios (Deutsche Post), diversas empresas, as entidades de classe dos advogados, as representações de consultores fiscais<sup>7</sup>.

Curiosamente, há que se ressaltar que nos Estados Unidos da América o desenvolvimento e a expansão das infra-estruturas de chaves públicas se deu de forma bastante desorganizada, de sorte que hoje em dia são diversas as ICPs em funcionamento naquele país, com base tanto em iniciativas governamentais quanto em iniciativas privadas.

As razões desse fenômeno são diversas, sendo que um dos motivos principais é o fato de que a autonomia dos estados federados fez com que cada unidade da federação editasse a sua própria lei sobre assinaturas digitais e matérias afins, sem que houvesse uma harmonia principiológica permeando esses diplomas.

Todavia, cientes de que *"PKI is no good if you are only talking to yourself"*<sup>8</sup>, os norte-americanos há alguns anos promoveram a iniciativa do projeto *Federal Bridge Certification Authority*, que tem por escopo fundamental viabilizar a intercomunicação entre os titulares de pares de chaves cujos respectivos certificados sejam provenientes de autoridades certificadoras diversas. Em que pese os esforços, os próprios envolvidos no projeto têm reconhecido que a iniciativa se transformou numa "empreitada que tem sido marcada pelo lento progresso"<sup>9</sup>.

Daí a razão de ser mais racional e de resultados certamente melhores à implementação, desde o princípio, de uma ICP nacional.

Outro aspecto é que, havendo uma ICP mais abrangente, como são a brasileira e a alemã, torna-se bem mais viável e atraente a celebração de acordos internacionais de reconhecimento recíproco de certificados digitais, o que possibilitará transações eletrônicas internacionais mais seguras, entre empresas e entre consumidores e empresas<sup>10</sup>.

No Brasil, as normas a serem cumpridas e observadas pelo ITI e por todas as entidades integrantes da ICP-Brasil são deliberadas pelo Comitê Gestor, que tem na Comissão Técnica Executiva (COTEC) o seu braço técnico e órgão consultivo que examina todas as proposições a serem apreciadas<sup>11</sup>.

Dos estudos da COTEC, e das contribuições advindas da consulta pública realizada em 2001, é que se originaram os documentos básicos da ICP-Brasil, posteriormente aprovados pelo Comitê Gestor. Até o momento, já foram deliberadas cerca de trinta resoluções, mas aquelas que poderiam ser consideradas o núcleo duro normativo são as Resoluções de nºs 1, 2, 7 e 8 (respectivamente, Declaração de Práticas de Certificação da AC Raiz, Política de Segurança da ICP-Brasil, Requisitos mínimos para as Políticas de Certificados e Requisitos mínimos para as Declarações de Práticas de Certificação).

3. Interoperabilidade e ICP-Brasil: interoperabilidade objetiva e interoperabilidade subjetiva

Este conjunto de resoluções e a Medida Provisória nº 2.200-2 contém a base técnica e jurídica da infra-estrutura, e tem como um dos escopos principais garan-

tir a interoperabilidade na utilização dos serviços relacionados à certificação digital, a partir do estabelecimento de padrões<sup>12</sup>. E a idéia que influenciou a criação da ICP-Brasil foi justamente a de constituir uma infra-estrutura para a coletividade<sup>13</sup>, para toda a sociedade, tornando mais facilitada a comunicação entre os titulares de certificados digitais. Evidente que nem tudo está feito, pelo contrário, a implementação das assinaturas digitais certamente trará dificuldades e problemas e mostrará que há muito por fazer para que efetivamente se atinja a desejada interoperabilidade, que deve ser encarada como um desafio, algo em constante construção, e não como algo pronto e acabado, que tenha se esgotado com a simples edição do conjunto normativo mencionado.

E um desses desafios é o relativo à compatibilidade dos cartões inteligentes, leitoras e softwares. Esse ponto é fundamental. Há que se padronizar esses instrumentos, a fim de que, na prática, se tenha a possibilidade de assinar digitalmente, bem como verificar as assinaturas digitais a partir de qualquer equipamento. Por isso, há que se louvar a iniciativa do Instituto Nacional de Tecnologia da Informação em constituir, por meio da Portaria nº 33, de 8 de abril de 2003, grupo de trabalho "para o estudo de padrões com especificações mínimas para o uso de hardwares e softwares na Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil", que redigirá "minuta de resolução que será submetida ao Comitê Gestor da ICP-Brasil" e que tem como uma das finalidades "colaborar na interoperabilidade desses dispositivos"<sup>14</sup>. Realmente, este é um ponto essencial, mas não é só a partir dele

que se explica a interoperabilidade, que, a meu juízo, não termina aí. O que se verifica é que, além dessa interoperabilidade, que eu proporia a denominação de interoperabilidade operacional, formal, técnica ou objetiva, existe uma outra interoperabilidade, que se poderia cunhar de interoperabilidade substancial ou subjetiva. Enquanto que a primeira tem em mira a operação em si, ou seja, a própria criação da assinatura digital e a sua posterior verificação pelo destinatário do documento eletrônico, a segunda, a interoperabilidade subjetiva, vai um pouco além, ela invoca um fundo comum principiológico de índole normativa que faz com que os indivíduos envolvidos na comunicação ou transação eletrônica, seja como signatário, seja como *relying party*, confiem na utilização do serviço, sentindo-se seguros não só aqui e agora, ou seja, no momento da utilização do certificado digital, mas para trás e para frente, isto é, antes e depois de efetuada a transação eletrônica. A preocupação ora enfocada se dirige a aspectos outros, como os relativos aos critérios observados para identificar os titulares de certificados, à forma de geração do par de chaves criptográficas, direitos e obrigações das partes (deveres de indenizar, de contratação de seguro, etc.) e muitos outros que sustentam e regulam a operação técnica da utilização da assinatura digital.

O que se quer dizer com isso é que não basta que os dispositivos de criação e de verificação das assinaturas funcionem aqui e agora. Da mesma forma, não basta que todos os indivíduos envolvidos na transação ou na comunicação utilizem o padrão do formato do certificado X.509. Pre-

tender que a interoperabilidade se resolva apenas a partir da utilização disseminada do padrão X.509 é, sem dúvida, analisar o problema de forma bastante superficial e com total desconhecimento da magnitude envolvida nessa questão.

Por isso, dentre outras coisas, é importante que se tenha confiança de que aquele indivíduo que assinou digitalmente foi corretamente identificado pela autoridade de registro. Assim, Pedro deverá ser realmente Pedro, e não João. Aqui, portanto, vai um primeiro princípio, de suma importância, que é o da identificação do indivíduo mediante a sua presença física<sup>15</sup>, no sentido de tentar evitar, o máximo possível, as fraudes.

Outra norma importantíssima é a da geração do par de chaves pelo próprio titular do certificado, que tem por evidente finalidade evitar a alegação de rejeição da autoria de determinado documento eletrônico pelo titular do certificado, alcançando-se, assim, o denominado não-repúdio<sup>16</sup>. Poder-se-ia citar também as normas referentes ao tempo limite para revogação dos certificados e a frequência de emissão da Lista de Certificados Revogados (LCR)<sup>17</sup>.

Por outro lado, para que a interoperabilidade efetivamente se realize, é preciso que as aplicações que requeiram a utilização da certificação digital não restrinjam o acesso a certificado digital específico, isto é, emitido por apenas uma das autoridades certificadoras. Isso, evidentemente, para os casos de “aplicações voltadas para atendimento ao público em geral, assim considerados, dentre outros, os consumidores,

os contribuintes, os cidadãos, os beneficiários do sistema de saúde, do FGTS, da seguridade social (...)”<sup>18</sup>. Essa norma tem forte conotação de proteção do consumidor, para evitar, na medida do possível e da razoabilidade, que para cada aplicação se tenha que utilizar um certificado digital diferente.

Sem a pretensão de fazer um elenco exaustivo de todas essas regras que constituem esse fundo principiológico normativo comum, chama-se a atenção para um outro ponto, pouco falado, mas de fundamental importância, que é o contido no item 6.3.1 da Resolução nº 7 da ICP-Brasil, que se refere à obrigação das autoridades certificadoras de armazenar, pelo prazo mínimo de 30 anos, as chaves públicas dos titulares de certificados digitais já expirados. Esse é um item essencial. Por meio da observância dele, é possível que se verifique a assinatura digital muito tempo depois de ter sido assinado o documento eletrônico, o que é de suma importância naqueles casos em que se fará necessária a sua posterior apresentação e conferência. Esse prazo é mínimo, por vezes pode haver a necessidade de que as chaves públicas sejam armazenadas por tempo ainda maior<sup>19</sup>. O lapso temporal de 30 anos é devido ao prazo máximo prescricional que poderia haver na legislação. Vale lembrar que, na Alemanha, o certificado de uma autoridade certificadora credenciada é considerado imprescindível, entre outros tantos aspectos, porque há esta obrigação de armazenamento das chaves públicas, que também é de 30 anos a contar do primeiro dia do ano seguinte ao da expiração do certificado digital<sup>20</sup>. Para as entidades que não são creden-

ciadas, a obrigação é de, no mínimo, 5 anos<sup>21</sup>.

Conforme referido, existe, na ICP-Brasil, um sem-número de outros aspectos, tão ou mais importantes do que os alinhados, como a obrigatoriedade de contratação de seguro pelas autoridades certificadoras, segurança dos dispositivos de armazenamento da chave privada, segurança do ambiente físico das autoridades certificadoras, vedação do denominado *key-escrow*, procedimentos de auditoria e de fiscalização, que acabam por constituir esse fundo principiológico comum, de índole normativa, e que geram, ou devem gerar, nos indivíduos integrantes da estrutura e naqueles que utilizam ou conferem os certificados digitais, um sentimento de segurança, e, mais do que isso, a *confiança*, que talvez seja a palavra-chave de uma infra-estrutura de chaves públicas e que os alemães bem souberam utilizar ao qualificarem a sua, denominando-a de *Kette des Vertrauens* (cadeia, ou rede da confiança).

É verdade que nem todos os indivíduos, ao utilizarem o seu certificado digital, estarão conscientes de todos esses aspectos, e também é verdade que fraudes e erros ocorrerão, pois nenhum sistema é de todo imune à falhas, mas o importante é que os usuários tenham um mínimo de segurança e de discernimento de que o máximo foi feito para se evitar problemas, e que se, porventura, algum venha a ocorrer, alguém será responsabilizado, como na hipótese de uma autoridade certificadora encerrar definitivamente as suas atividades, caso em que outra entidade deverá assumir as suas funções, pelo menos no que toca aos certificados digitais já emitidos<sup>22</sup>. Oportuno des-

taçar aqui, também, a importância de o Estado regular e fiscalizar esse incipiente, mas promissor, mercado, haja vista que os consumidores ainda não têm um mínimo de consciência acerca do que significa e do que não significa qualidade no que toca à prestação dos serviços de certificação digital. Quanto a esse aspecto, recomendo expressamente a leitura da resposta número um das FAQs, contida na página da *Regulierungsbehörde für Telekommunikation und Post*<sup>23</sup>, onde é feito um paralelo entre as exigências dos consumidores, motoristas de automóveis, de vinte e cinco anos atrás, e as de hoje.

Assim, verifica-se que para haver interoperabilidade não basta que o simples procedimento da assinatura digital do momento, do aqui e do agora, funcione. É necessário que todo o sistema tenha funcionado satisfatoriamente desde a primeira identificação do primeiro titular de certificado e que continue a funcionar, indefinidamente, de forma razoável. Além disso, será muito difícil que se estabeleçam transações ou comunicações virtuais que demandem segurança se as pessoas naturais ou jurídicas não estiverem regidas e protegidas por um fundo principiológico comum que, além de lhes impor deveres, lhes transmita confiança na utilização do meio eletrônico. Em suma, é importante que os documentos básicos das autoridades certificadoras (as PC e DPC) contenham um mínimo de similaridade quanto aos aspectos primordiais dos serviços, a fim de que seja possível a “conversação”. Daí a importância dessa “outra perna” da interoperabilidade, que enfeixa todos os aspectos citados, que poderia ser chamada, para efeitos ilustrativos, de interopera-

bilidade substancial ou subjetiva.

#### 4. Conclusões

(a) a interoperabilidade é um atributo necessário de qualquer infra-estrutura que pretenda atingir a coletividade, e consiste, numa acepção geral, na capacidade que têm os aparelhos ou equipamentos que fazem parte dessa infra-estrutura de comunicarem-se entre si, independentemente de sua procedência ou do seu fabricante; assim como uma infra-estrutura ferroviária necessita de padrões, uma infra-estrutura de chaves públicas também deverá estabelecer *standards* mínimos a serem observados pelos seus integrantes;

(b) neste sentido, o modelo da ICP-Brasil, previsto na Medida Provisória nº 2.200-2, e que é idêntico ao adotado pela Alemanha e outros países, deve ser considerado razoável, uma vez que, com o estabelecimento de uma espinha dorsal normativa comum, resta bastante facilitada a interoperabilidade;

(c) a noção de interoperabilidade aplicada a uma infra-estrutura de chaves públicas não se esgota no simples funcionamento da criação da assinatura digital, numa ponta, e de sua verificação na outra; portanto, ao lado dessa interoperabilidade objetiva, formal ou operacional, há que se referir à interoperabilidade subjetiva ou substancial, que invoca um fundo principiológico comum, expressado nas normas e padrões, que conferem as necessárias confiança e segurança aos usuários dos serviços de certificação digital;

(d) enfim, a interoperabilidade é algo a ser permanentemente

construído, um desafio constante, que exige esforço de todos os envolvidos. Há, como se sabe, muito a ser feito na ICP-Brasil. Por fim, eu chamaria a atenção para um último ponto que exigirá regulação num futuro bem próxi-

mo e que, salvo meu desconhecimento, pouco tem sido abordado no Brasil com vistas a sua inserção na ICP-Brasil, que é o atinente à necessidade de se proceder a reassinatura (aposição de nova assinatura digital) nos do-

cumentos eletrônicos que necessitam arquivamento por longo período de tempo, tendo em vista que “os procedimentos de criptografia podem perder, ao longo dos anos, seus atributos de segurança”<sup>24</sup>.

---

## Notas

<sup>1</sup> A definição do vocábulo “infra-estrutura” do Dicionário Aurélio, no que toca à área de urbanismo, é a mais adequada à acepção ora enfocada, *in verbis*: “Numa cidade, o conjunto das instalações necessárias às atividades humanas, como rede de esgotos e de abastecimento de água, energia elétrica, coleta de águas pluviais, rede telefônica e gás canalizado.” Vide *Novo Aurélio Século XXI: o dicionário da língua portuguesa*, Aurélio Buarque de Holanda Ferreira. Rio de Janeiro: Nova Fronteira, 1999.

<sup>2</sup> Obra cujo subtítulo é *Concepts, Standards, and Deployment Considerations*. Indianapolis: New Riders, 1999. p. 27.

<sup>3</sup> Ob.cit. p.27-28.

<sup>4</sup> É o que se depreende do parágrafo segundo da Medida Provisória nº 2.200-2, de 24 de agosto de 2001: “O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação de autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados digitais não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento”.

<sup>5</sup> A comparação com a árvore invertida está na obra citada, página 134.

<sup>6</sup> Pelo que se tem notícia, além de Brasil e Alemanha ([www.regtp.de](http://www.regtp.de)), Coreia do Sul ([www.rootca.or.kr](http://www.rootca.or.kr)), Índia ([www.cca.gov.in](http://www.cca.gov.in)), Áustria ([www.rtr.at](http://www.rtr.at)), México e Japão apresentam o mesmo modelo hierárquico com uma entidade de direito público desempenhando o papel de Autoridade Certificadora Raiz. Quanto ao Japão e sua forte inspiração alemã, vide “*Japanische Signaturgesetzgebung – Auf dem Weg zu „e-Japan*”. Artigo de autoria de Alexander Roanagel e T. Yonemaru, Revista Multimedia und Recht, nº 5, volume 12, p. 798 – 806.

<sup>7</sup> Conferir em [www.regtp.de](http://www.regtp.de)

<sup>8</sup> São as exatas palavras proferidas por Peter Alterman, diretor de operações do escritório de pesquisa extra-mural do Instituto Nacional de Saúde dos Estados Unidos da América. Declaração contida no artigo PKI at the crossroads, de autoria de Jennifer Jones, capturado, em <http://www.fcw.com/fcw/articles/2002/0624/tec-pki-06-24-02.asp>, no dia 04.07.2002.

<sup>9</sup> Idem anterior. O texto original diz o seguinte: “*Years in the works, a federal effort to link the public-key infrastructures (PKIs) of agencies has proved quite an undertaking and has been marked by that appears to be rather slow progress*”.

<sup>10</sup> O art. 4º, inciso VII, da MP 2.200-2, determina que compete ao Comitê Gestor da ICP-Brasil “identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais”.

<sup>11</sup> Sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira e a Comissão Técnica Executiva, vide o Decreto nº 3.872, de 18.07.2001. Sobre a necessidade de a COTEC manifestar-se previamente sobre todas as matérias a serem apreciadas pelo Comitê Gestor, vide art. 4º, parágrafo terceiro, inciso I do aludido decreto.

<sup>12</sup> De maneira que foi absorvida e ampliada, pela ICP-Brasil, a iniciativa da ICP-Gov de que tratava o revogado Decreto nº 3.587, de 5.09.2000.

<sup>13</sup> Vide os considerandos da Portaria nº 33, de 08.04.2003.

<sup>14</sup> Esta exigência foi determinada no art. 7º da Medida Provisória nº 2.200-2 e reafirmada no item 3.1.9 da Resolução nº 7.

<sup>15</sup> Vide o parágrafo único do art. 6º da MP 2.200-2 e item 6.1.1 da Resolução nº 7. O não-repúdio é uma presunção relativa de que aquele que assinou digitalmente, a princípio, estará vinculado à declaração de vontade manifestada. Por ser uma presunção relativa ou *juris tantum*, é possível a prova em contrário. Por exemplo, o suposto autor da manifestação de vontade poderá provar que foi coagido a assinar determinado documento eletrônico, e, assim, fazer cessar a presunção de autoria. Todavia, tudo dependerá da análise do conjunto probatório, e se o caso chegar ao Poder Judiciário, o magistrado competente deverá investigar fatos como, se após cessada a coação, o coagido tomou as devidas cautelas para comunicar ao destinatário da mensagem sobre o ocorrido, a fim de paralisar eventual execução contratual (comunicando até mesmo a necessidade de revogação do certificado perante a autoridade certificadora). Enfim, existem infinitas possibilidades de combinação de fatos que deverão ser analisados com prudência e cuidado pelo juiz.

<sup>16</sup> Estes procedimentos estão estabelecidos nos itens 4.4.3 a 4.4.9 (vide também anexo I), da Resolução nº 7.

<sup>17</sup> Como dispõe o item 1.3.4 da Resolução nº 7, que assim continua “(...), que aceitarem certificados de um determinado tipo previsto pela ICP-Brasil, devem aceitar todo e qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitidos por qualquer AC integrante da ICP-Brasil”.

<sup>18</sup> Casos de documentos eletrônicos que tenham de ser arquivados por prazos de tempo ainda maior. Por exemplo, caso os registros de imóveis e os arquivos de registros civis venham a armazenar os seus registros de forma eletrônica, o armazenamento das chaves públicas certamente deverá ser por prazo indeterminado.

<sup>19</sup> Quanto a este aspecto, vide o item 2 do parágrafo quarto do Decreto de Assinatura alemão, de 16.11.2002, o denominado *Signaturverordnung*. Na doutrina alemã, quanto a este aspecto e quanto à valorização e à indispensabilidade do certificado digital fornecido por autoridade certificadora credenciada perante a *Regulierungsbehörde für Telekommunikation und Post*, vide Alexander Roanagel, no artigo **Rechtliche Unterschiede von Signaturverfahren**, publicado na Revista Multimedia und Recht, nº 4, 2002, p. 215-222.

<sup>20</sup> Vide o item 1 do parágrafo quarto da *Signaturverordnung*.

<sup>21</sup> Daí ser de extrema importância o disposto no parágrafo 3º do art. 11 do Projeto de Lei nº 7.316/2002, uma vez que dispõe que, em último caso, a própria AC Raiz, como a âncora de confiança do sistema, acaba por assumir os documentos relativos aos certificados já emitidos por entidade que venha a encerrar as suas atividades.

<sup>22</sup> [www.regtp.de](http://www.regtp.de)

<sup>23</sup> Tradução livre que fiz de trecho do excelente artigo de Ralf Brandner, Ulrich Pordesch, Alexander Roanagel e Joachim Schachermayer, sob o título **Langzeitsicherung Qualifizierter Elektronischer Signaturen** (A proteção duradoura das assinaturas eletrônicas qualificadas), que versa especificamente sobre o tema, publicado na Revista DuD – Datenschutz und Datensicherheit, nº 2/2002, p. 97-103.



# A privacidade na ICP-Brasil



## Alexandre Rodrigues Atheniense

Advogado. Sócio da Aristóteles Atheniense Advogados S/C. Coordenador do Curso de atualização de Direito na Informática na PUC Minas Virtual. Presidente da Comissão de Informática do Conselho Federal da Ordem dos Advogados do Brasil. Presidente da Comissão de Informática da Seccional de Minas Gerais da Ordem dos Advogados do Brasil. Vice-presidente jurídico da Sucsus-MG.

## RESUMO

O artigo apresenta a delimitação do conceito de privacidade, assim entendido pela doutrina clássica do Direito. Procede-se, então, a uma análise da tutela constitucional da intimidade e da vida privada. Clarifica-se, para fins meramente didáticos, a distinção existente entre os termos "intimidade" e "vida privada". São traçadas algumas linhas a respeito da ideologia da infra-estrutura de chaves públicas, implementada pela Medida Provisória nº 2.200-2, analisando a doutrina nacional a seu respeito. Parte-se, assim, para as críticas a serem feitas em relação à instituição de um certificado único para os usuários e à possibilidade de se realizar análise de tráfego dos certificados revogados pelas autoridades certificadoras.

*Palavra-chave:* privacidade (na ICP-Brasil).

### 1. O conceito do direito à privacidade

O direito à privacidade tem consistido em objeto de estudo de inúmeros juristas ao longo dos anos. No entanto, revela-se, em certa medida, ingrata, a difícil tarefa a que alguns se propunham de delimitar sua abrangência na vida social.

Cumprido esclarecer, portanto, antes de adentrarmos à análise conceitual desse direito, a própria etimologia da palavra, que deriva do termo latino *privatus*, e que,

segundo SAMPAIO (1998)<sup>1</sup>, significa *fora do Estado, pertencente à pessoa ou ao indivíduo mesmo*.

É assim que podemos conceituar a privacidade como uma faculdade inerente a todo e qualquer indivíduo de manter fora do alcance de terceiros o conhecimento sobre fatos inerentes a sua própria pessoa ou atividades particulares.

É o direito à privacidade, destarte, um direito eminentemente subjetivo, delimitado pela própria

cognição do indivíduo. Nesse sentido, assinalou a melhor doutrina norte-americana ao decidir, no caso *Katz vs. United States*, que o direito à privacidade do indivíduo não se estenderia apenas à sua casa e documentos, mas também a qualquer lugar no qual ele pudesse ter *razoável expectativa de privacidade*.

A privacidade concebida em seu sentido lato ainda pode ser entendida como "o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito" (SILVA, 2001)<sup>2</sup>.

O direito à privacidade é, dessa maneira, excepcional, na medida em que consiste num direito negativo, ou seja, expresso exatamente pela não-exposição a conhecimento de terceiro de elementos particulares da esfera reservada do titular (BITTAR, 2001)<sup>3</sup>. Mera espécie do direito à privacidade é o direito à autodeterminação informativa, criação da doutrina espanhola, e comentado por COSTA (2001)<sup>4</sup>:

"Passados pouco mais de 100 anos daquela publicação, vivemos hoje também a necessidade da criação de um novo direito do cidadão, curiosamente nascido daquele direito à privacidade, que acabou consagrado no último século, fundado nas mesmas razões do desenvolvimento tecnológico e de métodos comerciais,



agora por causa da informática e da telemática, e pautado naquela mesma expressão singela, mas marcante, de que nos deixem em paz, direito esse que se constitui na proteção do cidadão em face do tratamento automatizado de seus dados (...).”

No entanto, decerto que a abrangência desse direito não é incondicional. GODOY (2002)<sup>5</sup>, citando CALDAS, nos lembra que: “(...) a vida privada do indivíduo presente, necessariamente, uma face pública, consubstanciada nas contingências da vida de relações, da vida profissional de alguém, de sua obrigatória exposição, (...) essa exposição será maior, a limitar a privacidade, de acordo com a atividade da pessoa (...)”.

Assim é que podemos concluir que o direito à privacidade será tanto menor quanto maior seja a notoriedade ou publicidade do indivíduo, estando certos de que a liberdade de imprensa também é um direito resguardado pela nossa Constituição.

## 2. A proteção constitucional da intimidade e da vida privada

A Constituição Federal consagrou, em seu artigo 5º, inciso X, que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Não obstante, temos a privacidade como valor constitucional inserto no seletor rol de direitos e garantias fundamentais da pessoa humana, sem os quais não se poderia assegurar uma convivência digna e igualitária do tecido social. Nesse particular, vale a

ressalva do art. 60, §4º da Lei Magna que erigiu tal garantia à condição de cláusula pétrea.

Custosa é a distinção doutrinária ao analisar a disparidade entre os termos intimidade e vida privada, inculpidos no rol de garantias individuais de nossa Carta Magna. A doutrina converge, conforme assinala GODOY (2002)<sup>6</sup>, no sentido de que, quando se procura diferenciar vida privada e intimidade do indivíduo, estabelece-se, entre os conceitos, verdadeira relação de gênero e espécie.

E continua, agora citando SERRANO: “(...) privacidade qualificada, na qual se resguarda a vida individual de intromissões da própria vida privada, reconhecendo-se que não só o poder público ou a sociedade podem interferir na vida individual, mas a própria vida em família, por vezes, pode vir a violar um espaço que o titular deseja manter impenetrável mesmo aos mais próximos, que compartilham consigo a vida cotidiana”.

Em que pesem os argumentos de CASTRO (2002)<sup>7</sup> e SZANIAWSKI (1993)<sup>8</sup>, entendemos ser mera dedução lógica o entendimento de que a intimidade consiste em uma vertente do direito à vida privada, estando ambos previstos no bojo da Norma Constitucional em razão de má-técnica legiferante.

De acordo com o *iter* até aqui traçado, resta claro que a privacidade há de ser assegurada independentemente do meio escolhido para a prática de quaisquer atos jurídicos, inclusive o eletrônico, ora objeto desta análise.

Nesse íterim, não podemos entender a privacidade como o direito de estar só, há anos

conclamado pela doutrina anglo-saxônica, mas, sim, como um direito de manter-se, e à sua propriedade, fora do controle de terceiros, o que englobaria, necessariamente, o liame residual competente a cada indivíduo de impedir o acesso e a divulgação de informações sobre sua vida privada.

## 3. O direito à privacidade e sua tutela jurídica

O desenvolvimento de sistemas informáticos tem feito com que a busca pela tutela jurídica efetiva dos direitos da personalidade seja posta em evidência. Assim, podemos notar uma tendência à disciplina desses direitos em alguns códigos modernos, tais quais o italiano (artigos 5 a 10) e o português (artigos 70 a 81).

BITTAR (2001) assinala que *incursões* na vida privada, especialmente ditadas pela evolução da tecnologia e das comunicações, têm exigido o reconhecimento expresso desses direitos e a sua regulamentação, para garantir-lhes proteção no âmbito privado.

No Código Civil Brasileiro de 2002, deixou, o legislador, de tratar do direito à intimidade de forma precisa, limitando-se a estabelecer, em seu artigo 21, que a vida privada é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

A privacidade dos indivíduos é resguardada, portanto, não só em relação a fatos inerentes à sua vida privada, profissional e familiar, mas, também, em relação às suas informações pessoais. Tal qual é a importância dessa proteção, que o Código de Defesa

do Consumidor tutelou, em seu artigo 13, incisos X a XV, algumas condutas consideradas ilícitas em relação à manipulação de informações dos consumidores, quais sejam: impedir ou dificultar o acesso gratuito do consumidor a informações em cadastros, fichas ou registros de dados pessoais (...); elaborar cadastros de consumo com dados irreais ou imprecisos; deixar de comunicar ao consumidor, no prazo de cinco dias, as correções cadastrais por ele solicitadas; etc.

Não obstante a tutela jurídica das informações no âmbito privado, previu, a Constituição Federal, ação mandamental destinada à ciência de informações contidas em bancos de dados pertencentes a entidades públicas ou de caráter público, o *habeas data*.

Assim sendo, em se tratando de entidade ligada à Administração Pública, compete ao indivíduo um instrumento processual adequado como garantia dos direitos previstos no artigo 5º, inciso X (supracitado), XXXIII (direito a receber dos órgãos públicos informações de seu interesse particular) e XXXIV, “b” (obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimentos de situações de interesse pessoal).

Podemos notar, deste modo, que a tutela jurídica da vida privada, dada sua importância, encontra amplo respaldo seja na Constituição Federal, seja em lei infra-constitucional.

#### 4. A infra-estrutura de chaves públicas

O desenvolvimento econômico da internet certamente gera uma demanda para que os negócios

ali realizados sejam acobertados por um certo nível de segurança jurídica. Assim, surge a necessidade tanto da transmissão quanto do conteúdo das informações que trafegam na rede serem conservadas fidedignas para que possam servir de substrato tanto como prova de uma relação ocorrida quanto do convencimento do magistrado em uma eventual lide.

Dessa maneira, insurge-se falar sobre o papel de um terceiro, estranho à relação jurídica e portanto dotado de neutralidade, que detém poderes bastante para autenticar a identidade dos usuários e certificar a autenticidade tanto do conteúdo quanto da transmissão das informações em uma rede, *a priori*, insegura.

Tal qual é a opinião de BARRETO (2001)<sup>10</sup>:

“O papel dos terceiros certificadores insere-se perfeitamente nessa lógica de proporcionar segurança nas transmissões de dados via internet, sem que haja contudo ingerência no conteúdo de tais transmissões, bem como fornecer provas irrefutáveis que possam ser aceitas pelas partes em caso de litígio”.

Esse foi o espírito que motivou a edição da Medida Provisória 2.200-2, de 24 de agosto de 2001, que, dentre outros, instituiu a Infra-estrutura de Chaves Públicas no País.

De imediato, causa-nos estranheza que uma norma de tamanho impacto social seja elaborada por um ato do executivo, o que não deveria ocorrer em uma democracia representativa.

Em que pesem as críticas, instituiu a referida MP, o arcabouço fundamental concernente à vali-

dade jurídica do documento eletrônico. Através deste ato emanado pelo Poder Executivo, adotou-se uma estrutura centralizada – vertical – para a expedição de certificados eletrônicos.

Essa estrutura vertical, por sua vez, foi constituída sob a premissa de que um único certificado digital emitido para o usuário final se prestaria à prática de todos os atos da vida civil, facilitando, assim, a interoperabilidade entre os sistemas de certificação.

Com toda a *venia* às opiniões contrárias, entendemos que a adoção de um certificado único em nada facilitaria a interoperabilidade do sistema por absoluta inexistência de nexos causal entre os fatos.

A simples exigência da observância do credenciamento perante a AC-Raiz, por si só, representaria um risco social e um ônus insuportável a cargo do indivíduo.

A interoperabilidade entre as autoridades certificadoras é relacionada, sim, com o modelo de certificação adotado no mercado, tal como o X.509. BARRETO<sup>11</sup> traz a lume uma interessante ilustração: “Esse modelo é frequentemente referido como o modelo do cartão de crédito, na medida em que reflete o modelo comercial no qual a indústria do cartão de crédito se baseia. Na indústria do cartão de crédito, o que faz o comerciante aceitar o cartão de crédito apresentado pelo consumidor como forma de pagamento é o fato de o cartão ter sido emitido por um banco que ele conhece ou, ainda que o comerciante nunca tenha ouvido falar do banco que emitiu o cartão de crédito, esse banco terá sido certificado por uma companhia de

cartões de crédito (...).

Do momento em que o comerciante conheça e confie na companhia de cartões de crédito, ele poderá confiar no banco e no consumidor, e assim aceitar aquele cartão de crédito como forma de pagamento”.

E continua a referida autora: “A abordagem hierárquica do padrão X.509 oferece algumas vantagens, ao permitir que inúmeros certificados se relacionem a uma mesma raiz confiável”.

Mas o repúdio à estrutura do certificado único não se dá única e exclusivamente em razão de sua interoperabilidade, mas pela ameaça da instituição de um número único para cada indivíduo.

#### 4.1. A adoção do certificado único

A implementação de um certificado único envolveria a congregação de todas as informações acerca do indivíduo em um mesmo suporte, para se compatibilizar à ampla gama de serviços oferecidos no meio eletrônico. Nesse diapasão, assevera SILVA<sup>12</sup> que “o amplo sistema de informações computadorizadas gera um processo de esquadramento das pessoas, que ficam com sua individualidade inteiramente devassada”<sup>2</sup>.

Cumprir lembrar que, no final de 1995, a Comunidade Européia editou a diretiva 95/46 segundo a qual os “Estados Membros devem proteger os direitos e liberdades fundamentais das pessoas naturais, e em particular seu direito à privacidade em relação ao processamento de dados pessoais”.

Além disso, a própria Constitui-

ção Portuguesa vedou expressamente a adoção de um número único exatamente por antever os efeitos que poderiam ser causados pela prática deste ato, *in verbis*:

**“Art. 35.** Utilização da informática:

5 – É proibida a atribuição de um número nacional único aos cidadãos”.

Com efeito, a instituição de um certificado único, como quer implementar e regulamentar o CG – ICPBrasil, acabaria por comprometer a individualidade, intimidade e privacidade do cidadão. Não se pode elidir tal garantia sob a pretensa alegação de facilidade na utilização. Ademais, a instituição de uma AC Raiz (árvore única) garante o monopólio das informações por parte desta instituição, quando o mais seguro seria pulverizar as informações sobre o indivíduo em vários certificados, permitindo-se várias AC Raiz em um sistema floresta. A existência de uma única raiz é justificada pelo fato de permitir a interoperabilidade entre as ACs, entretanto, essa famigerada interoperabilidade pode ser alcançada através da adoção de padrões tecnológicos comuns (v.g. X.509).

A violação de um banco de dados contendo todas as informações pessoais (que será a tônica em um ambiente com certificado único) de um determinado indivíduo representaria um risco social insuportável na medida que sua vida privada poderia ser completa e indevidamente devassada. A utilização de aparatos informáticos facilita o tratamento da informação. Assim, esta violação não atingiria somente o âmbito de relacionamento do in-

divíduo com o órgão em questão, mas todo relacionamento daquele com a sociedade. Bem assevera GRECO (2000)<sup>13</sup> ao afirmar que: “numa sociedade complexa (...) o poder advém da posse de informações sobre pessoas, eventos ou coisas”<sup>3</sup>.”

A existência destes vários cadastros é, na verdade, uma garantia de que o indivíduo não terá sua vida devassada na medida em que dificulta o cruzamento de tantas informações complexas. Essa é a principal razão pela qual a instituição de um certificado único foi rechaçada pelos países europeus.

#### 4.2. A análise de tráfego

Outra questão controvertida em relação a ICP-Brasil concerne à análise de tráfego da consulta dos certificados revogados. Na utilização de um certificado digital, a verificação da lista de certificados revogados, mantida pela autoridade certificadora, poderia gerar, para diversos fins, um *log*, que em última análise pode fornecer algumas informações sobre aquele usuário.

Apesar de não ser capaz de acessar o conteúdo da mensagem em razão da certificação digital, o simples fato de ter ciência da comunicação seria capaz de ameaçar a privacidade dos usuários, uma vez que muitas informações podem ser obtidas através da análise do perfil (intervalo de tempo, tamanho, datas e horários das mensagens) dessas mensagens. A violação da privacidade do indivíduo poderia dar-se não pelo conhecimento do conteúdo que foi transmitido, mas de uma forma muito mais sutil, através do conhecimento da existência de comunicação

entre as partes. Afirma o professor SCHNEIER<sup>14</sup> que “often the patterns of communication are just as important as the contents of communi-

cation”<sup>4</sup>. Diante dessas considerações, reiteramos a crítica no sentido de não privilegiar o avanço tecnológico em detrimento dos direitos

e garantias fundamentais. E, ainda, compatibilizar a regulamentação da ICP Brasil com a ideologia constitucionalmente adotada.

---

## Notas

<sup>1</sup>. SAMPAIO, José Adércio Leite, *Direito a Intimidade e à Vida Privada*, Belo Horizonte: Del Rey, 1998, p.34

<sup>2</sup>. SILVA, José Afonso da Silva, *Curso de Direito Constitucional Positivo*, 19ª ed., São Paulo: Malheiros, 1997, p.209

<sup>3</sup>. BITTAR, Carlos Alberto, *Os Direitos da Personalidade*, 5ª ed. rev., atual., ampl. por Carlos Bianca Bittar. Rio de Janeiro: Forense, 2001, p. xx, p. xx, p. 108

<sup>4</sup>. COSTA, Marcos da, *Novos Ventos Digitais*, disponível em: [http://www.marcosdacosta.adv.br/documento.asp?ID\\_Documento=455](http://www.marcosdacosta.adv.br/documento.asp?ID_Documento=455) - acesso em: 15/05/2003

<sup>5</sup>. GODOY, Cláudio Luiz Bueno de, *A Liberdade de Imprensa e os Direitos da Personalidade*. São Paulo: Atlas, 2001, p.47;

<sup>6</sup>. Op. Cit. 5, p. 49

<sup>7</sup>. CASTRO, Mônica Neves Aguiar da Silva, Honra, *Imagem, Vida Privada e Intimidade em Colisão com Outros Direitos*. Biblioteca de Teses. Rio de Janeiro: Renovar, 2002, p.32

<sup>8</sup>. SZANIAWSKI, Elimar, *Direitos da Personalidade e sua Tutela*. São Paulo: RT, 1993, p. 132

<sup>9</sup>. Op. Cit. 3, p.35

<sup>10</sup>. BARRETO, Ana Carolina, *Assinaturas Eletrônicas e Certificação*, In: ROCHA FILHO, Valdir de Oliveira (coord.), *O Direito e a Internet*, Rio de Janeiro: Forense Universitária, 2002, p.44

<sup>11</sup>. Op. Cit. 10, p.48

<sup>12</sup>. Op. Cit. 2, p.212

<sup>13</sup>. GRECO, Marco Aurélio, *Internet e Direito*, 2ª ed., rev. e aum., São Paulo: Dialética, 2000, p.194

<sup>14</sup>. SCHNEIER, Bruce, *Secrets & Lies Digital Security in a Networked World*, Wilye Computer Publishing, 2000, p.34

---





# Tudo que você deve saber sobre certificação digital



## Jeroen van de Graaf

Pesquisador em criptografia há mais de 20 anos e doutor na área pela Universidade de Montreal, Canadá. Atualmente, trabalha como pesquisador na UFMG e atua como consultor autônomo através da sua empresa, a VDG-InfoSec.

## RESUMO

No mundo convencional de papel, estamos acostumados às propriedades de autenticidade, integridade e não-repúdio de documentos que, juntas, criam a fé indispensável para quase todos os processos burocráticos. Para um mundo digital (sem papel) dar certo, é necessário que essas propriedades continuem valendo. Este texto tenta explicar as noções básicas das novas tecnologias que estão surgindo para garantir a fé de documentos no mundo digital: a assinatura digital, o certificado digital e a infra-estrutura de chaves públicas, entre outros.

O texto tenta simplificar o máximo possível. No entanto, também não é desejável simplificar demais esse assunto complexo e fascinante; senão há o risco de perder a essência e enganar o leitor. Espero que minha tentativa contribua para a compreensão desse assunto por um público maior.

### 1. Assinar um documento convencional

Todo mundo já assinou um documento. A única observação importante é que cada assinatura é igual (em teoria), e que a ligação entre o texto do documento e a assinatura é o meio físico subjacente: o papel.

### 2. Assinar um documento digital

Uma assinatura digital é o resul-

tado de uma computação que tem duas entradas: um documento eletrônico e uma chave criptográfica e secreta. A computação embaralha todos os bits do documento e da chave, resultando numa seqüência de bits de tamanho fixo (normalmente 1024 bits). Esta é a assinatura digital, que é anexada ao documento original.

Uma assinatura digital tem a seguinte característica: sem acesso à chave secreta, é matematicamente impossível calcular qual a

seqüência de bits que constitui a assinatura digital. Claro, um forjador sempre pode “chutar” uma assinatura. Mas a probabilidade de acertar corresponde a ganhar a MegaSena 40 vezes seguidas, um evento tão improvável que, na prática, pode ser mesmo desconsiderado.

Observe que a autenticidade e o não-repúdio do documento assinado digitalmente se baseiam no conhecimento da chave: quem é dono da chave secreta é autor daquele documento. Portanto, o sigilo da chave é de suma importância. A integridade do documento se baseia numa outra característica do método da computação: se um bit do documento original for mudado, a assinatura sai completamente diferente; então, adulterar um documento assinado é impossível.

A assinatura digital se parece muito com a assinatura de punho, ou com o selo do mundo tradicional de papel. No primeiro exemplo, a chave secreta corresponde aos movimentos motores do assinante e, no segundo, é supostamente impossível recriar (ou seja, forjar) o selo, com sua estrutura fina de linhas, papel e tinta especial, etc. Como no mundo digital não há meio físico, a assinatura depende não apenas da chave, mas também do documento. Obviamente, deve ser assim; senão seria muito fácil cor-

tar uma assinatura digital de um documento e colá-la embaixo de um outro.

### 3. Verificar uma assinatura convencional

Até agora, falamos apenas sobre como assinar documentos, mas igualmente importante é como se verifica uma assinatura. Para entender mais tarde a verificação no mundo digital, é importante lembrar como isso funciona no mundo tradicional. São procedimentos tão cotidianos que é fácil se esquecer da sua importância. Para assinaturas de punho, é comum que um indivíduo se dirija pessoalmente a uma “autoridade” (um banco, um cartório). A autoridade confere a identidade da pessoa e cria uma ficha com dados pessoais e outros dados relevantes, e com a assinatura daquela pessoa. Em princípio, depois dessa visita, o indivíduo nunca mais precisa voltar. Quando um terceiro mostrar à autoridade um documento supostamente assinado por aquele indivíduo, ela procura a ficha, compara as duas imagens das assinaturas e dá um veredicto: a assinatura é válida ou não. Com selos, a situação é um pouco diferente, eles são emitidos por órgãos que já têm autonomia, então, não precisam de uma autoridade. Mas, nesse caso, também devem existir modelos para que terceiros possam comparar.

### 4. Verificar uma assinatura digital

No mundo digital, a verificação de uma assinatura é muito parecida, e em alguns pontos até mais flexível. Dada a chave secreta que é usada para assinar, é possível criar uma outra chave pública correspondente, que é usada na ve-

rificação da assinatura. Esse par de chaves tem uma característica surpreendente: mesmo conhecendo a chave pública, é matematicamente impossível calcular a chave secreta correspondente. Este modelo é conhecido como criptografia com chaves públicas. É diferente da criptografia convencional descrita nos livros de espionagem: neles, a chave para cifrar e decifrar deve ser a mesma, e ela não pode ser pública.

No mundo convencional, a chave secreta (também chamada de chave privada) corresponde aos movimentos motores do indivíduo, enquanto a chave pública corresponde à imagem da assinatura no papel, um dado que é público. E como no mundo convencional é necessário vincular a imagem da assinatura a uma identidade, é necessário que exista o mesmo procedimento no mundo digital. O indivíduo se dirige a uma autoridade com a sua chave pública (e talvez com outros documentos comprovando sua identidade), a autoridade confere a identidade da pessoa e cria uma ficha com os dados pessoais e a chave pública daquela pessoa.

Mas, em vez de guardar essa ficha no seu arquivo, a autoridade assina-a e publica-a na internet! É esse documento, contendo uma chave pública e os dados pessoais do seu dono, que é chamado um certificado digital. Ou seja, o certificado digital corresponde à ficha do cartório, carimbada pelo tabelião, publicada livremente. Um certificado digital não é sigiloso; ao contrário, pode e deve ser copiado e distribuído à vontade. A grande vantagem é que qualquer pessoa, em qualquer lugar no mundo com acesso à internet, pode verificar a assinatura.

Em outras palavras, verificar uma assinatura digital é parecido com verificar uma assinatura convencional: têm-se o documento assinado e o certificado digital; o último contém a identidade do assinante e a sua chave pública. E, através de uma segunda computação matemática, verifica-se se os dois conferem, ou seja, se a chave secreta usada para assinar o documento corresponde à chave pública no certificado.

### 5. Infra-estrutura de Chaves Públicas (ICP)

Note bem como funciona a cadeia de confiança no exemplo anterior: a identidade do assinante é garantida pela autoridade que emitiu (assinou) o certificado digital, comumente chamada Autoridade Certificadora (AC). Ou seja, é necessário que o verificador conheça a chave pública daquela AC para verificar se o certificado foi realmente assinado por ela. É nesse ponto que as coisas se complicam.

Como existem milhares de bancos e cartórios geograficamente espalhados no Brasil e no mundo, é claro que devem existir milhares de ACs. Mas é inviável que um verificador conheça todas as chaves públicas dessas autoridades. Portanto, por motivos de escalabilidade, existem “meta-autoridades”, que credenciam autoridades intermediárias, que emitem certificados a indivíduos.

O resultado é uma hierarquia de autoridades certificadoras: existe apenas uma AC-Raiz cujo único papel é emitir certificados para suas AC-intermediárias. Elas, por sua vez, emitem certificados para os indivíduos ou entidades pertencentes à hierarquia. Um sentido do termo Infra-estrutura de Chaves Públicas (ICP) é essa hierar-

quia (ou árvore) de certificação. Por exemplo, na ICP-Brasil há uma AC-Raiz e seis ACs-Intermediárias de primeiro nível: a Presidência da República, a Serasa, a Receita Federal, o Serpro, a Caixa Econômica Federal e a CertiSign.

Aliás, existe um outro uso da sigla ICP (PKI=Public Key Infrastructure, em inglês), o que cria bastante confusão. Como deve ser óbvio, existe uma quantidade enorme de padrões, software, hardware, procedimentos e documentos para essa tecnologia funcionar. O termo Infra-estrutura de Chaves Públicas (ICP), no sentido amplo, é usado também para se referir a esse conjunto, à tecnologia em geral.

Felizmente, existe um padrão adotado mundialmente (PKIX-X.509) e existe software livre para construir uma ICP (hierarquia). Por exemplo, o meu notebook contém um software para criar uma ICP funcional. No entanto, esse programa só serve para pesquisa, não é uma solução viável para gerenciar uma ICP com centenas de certificados. Mesmo assim, há uma implicação importante aqui: qualquer pessoa pode criar uma ICP. A padaria na esquina, o Minas Tênis Clube, a UFMG, o Estado de Minas Gerais, todo mundo pode emitir certificados. Então, se não houver impedimentos técnicos para emitir certificados, qual é a credibilidade (o valor) de um certificado?

## 6. A credibilidade de certificados

Nesse contexto, uma outra comparação com o mundo tradicional é muito interessante. Nossa carteira é cheia de documentos

que atestam nossas credenciais: carteira de identidade, carteira de motorista, cartões de crédito, carteirinha da biblioteca da UFMG, carteirinha da videolocadora, carteirinha de seguro de saúde, etc., etc. A credibilidade dessas não depende do documento em si, mas da política de quem o emitiu. Por exemplo, a credibilidade de um cartão American Express Platinum é diferente da do cartão Carrefour. E a carteira de identidade tem uma grande credibilidade para terceiros, porque todo mundo sabe que há um processo rigoroso por trás para consegui-la, enquanto a carteirinha da videolocadora não tem validade nenhuma porque todo mundo consegue facilmente.

Com certificados digitais é igual: a sua credibilidade depende completamente da política adotada pela autoridade certificadora emissora. Por exemplo, existe um site na internet que emite certificados automaticamente, sem verificação nenhuma e, portanto, sem credibilidade nenhuma, mas mesmo assim é útil para testes. Existem empresas que emitem um certificado a qualquer cidadão com nome, CPF e título de eleitor, após a verificação desses dados, cobrando uma taxa de 100 reais anual. E para ser AC-intermediária subordinada à AC-Raiz da ICP-Brasil é necessário pagar centenas de milhares de reais como taxa (sem falar dos custos para montar uma sala-cofre, que custa milhões, para guardar a chave privada). Lembre-se que, em todos os casos, estamos falando de certificados que são simplesmente bits, nem possuem um holograma bonito. Repito, a credibilidade do certificado advém da credibilidade da AC. Aliás, introduzindo carteiras de

identidade, mudamos sutilmente de assunto. Em vez de discutir a assinatura digital, que provê autenticidade, integridade e não-repúdio de documentos, estamos discutindo identificação: como estabelecer a identidade de pessoas. E, em muitas situações, ela é importante, porque associada a ela estão privilégios e direitos, por exemplo, o direito de dirigir um carro. Ou seja, a identificação leva a uma autorização. A tecnologia ICP serve também para implementar a identificação e autorização das pessoas no mundo digital.

Ainda por cima, a mesma tecnologia também pode ser aplicada para proteger o sigilo de documentos e comunicações, mas, na maioria das situações, as organizações não se preocupam com o sigilo, e, sim, com a fé dos documentos e processos, ou seja, com as questões de autenticidade, integridade e não-repúdio de documentos, e identificação de pessoas.

## 7. O lado comercial da certificação digital

O valor econômico dessa tecnologia foi logo percebido nos anos oitenta, mas explodiu com a chegada da internet. Em particular, o certificado digital é um mecanismo poderoso para estabelecer uma identidade digital das pessoas. Como explicamos, ele serve para assinar documentos, e também para comprovar a identidade. As maioria das empresas que atua nessa área ganha dinheiro cobrando pela emissão de certificados. As empresas colocam um prazo de validade de um ano, normalmente, garantindo uma fonte de renda regular. Na realidade, muitas vezes elas deixam de explicar a seus clientes

que criar uma própria ICP poderia ser uma opção interessante, dependendo das circunstâncias.

## 8. A ICP-Brasil

A ICP-Brasil foi uma iniciativa do governo anterior com a intenção de unificar a certificação digital no Brasil. Ela passa a impressão de que deve existir uma única ICP no Brasil, com ela ao topo. A própria palavra “infra-estrutura” pode levar o leigo a crer nisto, inconscientemente fazendo a analogia com a rede elétrica num país. Porém, a analogia certa é com a telefonia celular: podem existir vários operadores de telefonia celular paralelamente.

Não é sempre preciso aderir à ICP-Brasil para usar a certificação digital, às vezes nem é aconselhável. Primeiro, se uma organização (pública ou privada) quer emitir certificados para uso interno, ela obviamente tem o direito de fazê-lo. Qual é o ganho de aderir à ICP-Brasil, cujas exigências de segurança são rígidas demais para muitas organizações, e cujas taxas são altas? Segundo, há a questão de autonomia: várias organizações não querem ou não podem se subordinar a um órgão do Poder Executivo Federal.

E terceiro, a Medida Provisória 2200-2, que criou a ICP-Brasil, inclui um parágrafo (10.2) dizendo que se duas partes concordarem em assinar documentos usando certificados emitidos por uma ICP que não pertence à ICP-Brasil, estes documentos têm valor jurídico.

Ou seja, para uso interno, ou para partes que entram em acordo, não há necessidade de usar a ICP-Brasil.

## 9. ICPs alternativas

Por estes motivos, e por motivos de pesquisa e educação, as universidades brasileiras, lideradas pela UFSC, a Unicamp e a UFMG, estão criando uma ICP independente. Através de um projeto da Rede Nacional de Desenvolvimento e Pesquisa (órgão de pesquisa do MEC e MCT), elas criaram em 2005 a ICP-EDU, uma ICP no âmbito acadêmico, baseada em software livre. A OAB já criou sua própria ICP.

Então, é provável que coexistirão várias ICPs; isto é inevitável. Pela mesma razão que todos nós temos uma grande variedade de carteiras, carteirinhas e cartões, refletindo nossas relações diversas com entidades públicas e privadas, teremos vários certificados diferentes emitidos por ICPs diferentes. Se isso levar a confusão, uma solução seria padronizar as políticas das ICPs por lei, não a imposição de uma única ICP.

## 10. A questão da privacidade

Pessoalmente, não acredito que a idéia de unificar todos esses certificados em um único, emitido pela ICP-Brasil, vá dar certo, porque combinar todos as funcionalidades requeridas por vários órgãos públicos é muito complicado.

Aliás, seria o grande sonho do Grande Irmão, um certificado único por cidadão: pode-se rastrear a vida digital de uma pessoa completamente. Essa questão da privacidade fez vários países desistirem de uma ICP nacional, mas no Brasil ninguém se parece preocupado; ainda não vi nenhuma proposta lidando adequadamente com esta questão.

## 11. Conclusão

Certificação digital é uma tecnologia muito promissora, pois ela permite implementar o não-repúdio e a identificação de pessoas jurídicas e físicas no mundo digital. Mas é uma tecnologia nova, e ainda há bastantes questões tecnológicas, econômicas, jurídicas e políticas a serem resolvidas.

Porém, o maior obstáculo é cultural: estamos todos apegados ao mundo do papel. Uma prova disso é que a primeira imagem que entra em nossa mente quando pensamos na palavra “documento” é a do papel, e não as informações escritas nele. Ou seja, o mundo digital traz uma separação de mídia e conteúdo que no mundo de papel não existia. Ainda mais forte: no caso de uma assinatura de punho, a ligação entre o conteúdo e a assinatura é estabelecida através da mídia; o papel é apenas intermediador, porém essencial na questão da autenticidade e, portanto, da validade jurídica.

Até que todo mundo se acostume ao documento eletrônico e confie na sua autenticidade, vai levar muitos anos, talvez décadas. É uma profunda mudança de paradigma.

# Certificação Digital - Uma Realidade em Minas



## Raymundo Albino

Engenheiro electricista e analista de suporte de sistemas, graduado pela PUC-MG. Atua como assessor técnico da Diretoria de Tecnologia e Produção da Prodemge, tendo passado pela Gerência de Redes e Superintendência de Produção. Participa atualmente do grupo de trabalho criado pelo governador para implantar a certificação digital no âmbito do Estado de Minas Gerais.



## Sérgio Daher

Engenheiro electricista e analista de suporte de sistemas, graduado pela PUC-MG. Atua como superintendente de Tecnologia e Suporte da Prodemge, já tendo exercido diversos cargos gerenciais na empresa. Participa do Grupo de Trabalho de Certificação Digital, instituído pelo Governo do Estado de Minas Gerais.

## RESUMO

O artigo dá uma visão global da necessidade do uso da certificação digital nas instituições, tanto públicas como privadas, especialmente devido ao uso crescente da internet em transações e relacionamentos entre empresas e cidadãos, buscando sempre garantir a Confidencialidade, Integridade e Disponibilidade das informações.

Em seguida, é feita uma explicação sobre conceitos de criptografia, assinatura digital e certificação digital, mostrando as principais aplicações já em uso no Brasil.

O artigo é concluído com a posição da certificação digital no Estado de Minas Gerais, mostrando o que já foi feito e as aplicações já eleitas para utilizarem os benefícios desta tecnologia nos órgãos e entidades estaduais, visando à agilização da máquina administrativa e à melhoria dos processos de relacionamento entre o Estado e o cidadão.

**Palavras-chave:** Certificação Digital (do Estado de Minas Gerais)

Com o crescente aumento de utilização da internet para o trâmite de documentos eletrônicos, verifica-se que as organizações, tanto públicas como privadas, estão cada vez mais preocupadas com a segurança e legalidade desses processos. Quanto à segurança no tráfego

e armazenamento de documentos eletrônicos, os aspectos que mais preocupam as organizações são: sigilo, integridade, autenticidade e não-repúdio. Quanto à legalidade, as preocupações se voltam para a validade jurídica e força probatória. Informações sigilosas são aque-

las que só podem ser acessadas pelo legítimo receptor do documento. A integridade é a garantia de que o documento recebido não está alterado ou fraudado. A autenticidade é a garantia de autoria do emissor ou aprovador do documento. O não-repúdio é a impossibilidade do emissor negar a realização da transação ou autoria. Quanto à legalidade, um documento ou processo eletrônico terá validade jurídica quando aceito como prova e força probatória e quando não puder ser impugnado em uma eventual contestação.

Hoje, a certificação digital, combinando aspectos tecnológicos e jurídicos, possibilita tratar a segurança e legalidade de documentos e processos eletrônicos com garantia de autenticidade, integridade, sigilo, não-repúdio e legalidade. Cresce a cada dia o número de empresas e organizações governamentais que, descobrindo as potencialidades da certificação digital, passam a implementar soluções baseadas nessa tecnologia, aumentando a segurança de seus processos.

## Criptografia

A inviolabilidade de informações sensíveis é uma preocupação constante da humanidade já há muitos séculos. Inúmeros mecanismos de codificação de informações foram



utilizados, com objetivo de reduzir a possibilidade de que adversários obtivessem informações secretas, através da captura de documentos em trânsito ou arquivados.

Historicamente, temos evidências da utilização de mecanismos criptográficos remontando à China antiga. Como exemplo, mostraremos a CIFRA DE CÉSAR, um pouco mais moderna, da época em que Júlio César governava o Império Romano. Este método foi concebido através da substituição posicional do alfabeto, utilizando uma chave que marca o deslocamento a ser adotado na codificação da mensagem. A seguir, mostramos um exemplo onde é utilizada a chave 6, ou seja, cada letra do alfabeto da mensagem original deverá ser substituída pela letra que estiver na 6ª posição anterior, para formar a mensagem cifrada:

**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**  
**U V W X Y Z A B C D E F G H I J K L M N O P Q R S T**

**CHAVE = 6**

**ORIGINAL SIGILO PELA CRIPTOGRAFIA**  
**CIFRADA MGACFIUJZ FVUXLCJNIALV CV**

Junto ao desenvolvimento da humanidade, métodos cada vez mais sofisticados foram desenvolvidos, sempre na disputa de uma verdadeira guerra: métodos mais sofisticados de cifragem contra métodos cada vez mais aperfeiçoados de decifragem.

O desenvolvimento da informática tem sido um grande aliado na guerra da criptografia, permitindo que sistemas extremamen-

te complexos de codificação possam ser desenvolvidos, assim como mecanismos de decodificação, também superpoderosos, possam ser concebidos e implementados.

O objetivo é alcançar condições onde mesmo os mais poderosos computadores tenham chances mínimas de decifragem de mensagens em prazos em que métodos administrativos de segurança possam ser implementados a custos razoáveis (troca sistemática de chaves).

O método mais eficaz conhecido é o modelo de chave pública utilizando exponenciação. Cada participante da estrutura possui uma chave secreta e uma chave pública. Assim sendo, uma mensagem, para ser enviada, é inicialmente criptografada pela chave do receptor, garantindo que só ele seja capaz de decifrar a mensagem

através de sua chave secreta. Este processo, utilizando uma chave de duzentos algarismos, dependeria 10 milhões de séculos de um computador capaz de 1 milhão de multiplicações por segundo para que o sigilo fosse quebrado.

O método pode também ser utilizado em sistemas de assinatura eletrônica, quando, então, um documento poderá ser enviado

eletronicamente com garantia de origem e destino.

Apesar da transcrição anterior ser datada de 1992, quando foi publicada na revista comemorativa dos 25 anos da Prodemge, época ainda anterior à realidade atual do mundo Web, demonstra-se atual nas técnicas da segurança da informação.

O que ocorreu nos anos que se seguiram foi a massificação da sua utilização através das aplicações de comércio eletrônico, hoje utilizado por toda a comunidade conectada à internet, seja para a compra de mercadorias e serviços, ou mesmo a consulta do saldo de uma conta corrente bancária através da Web.

O estágio atual da utilização das técnicas de criptografia no ambiente das transações eletrônicas se resume, na grande maioria das aplicações, à garantia da autenticidade do destino a que se conecta o usuário, assegurando-lhe que a instituição, na qual uma determinada transação está sendo efetuada, seja aquela que ele realmente deseja e espera, preservando também o sigilo das comunicações trocadas durante o procedimento.

O que nos avizinha é a identificação inequívoca também do usuário dos sistemas de informação, obtida através de certificados digitais pessoais, seja de pessoas físicas ou jurídicas, garantindo, desta forma, a impossibilidade do repúdio da realização das transações por elas originadas.

Tal realidade, em um futuro próximo, trará garantias adicionais a toda a comunidade envolvida com o mundo das transações eletrônicas, destino inexorável de toda a civilização.

# Sistema de Criptografia RSA

## O receptor da mensagem:

- > escolhe dois números primos,  $p$  e  $q$ , calculando  $n=p \cdot q$ ;
- > determina  $\phi(n) = (p-1) \cdot (q-1)$ ;
- > escolhe o expoente de codificação, tal que  $1 < e < \phi(n)$  e  $\text{mdc}(e, \phi(n)) = 1$ ;
- > determina o expoente de decodificação, tal que  $1 < d < \phi(n)$  e  $ed = 1 \pmod{\phi(n)}$ ;
- > publica o par  $(n, e)$ , que se diz a Chave Pública, mantendo secreto o par  $(n, d)$ , a Chave Privada.

## O emissor da mensagem:

- > converte a mensagem no número inteiro  $M$ ,  $0 < M < n$ , recorrendo a um “alfabeto digital”, por exemplo,  $A = 01$ ,  $B = 02$ ,  $C = 03$ , ...,  $Z = 26$ ;
- > obtém a chave pública  $(n, e)$  do destinatário;
- > converte o número  $M$  no número  $C$  através da fórmula de codificação:  
 $C = M^e \pmod{n}$ , onde  $M$  representa a mensagem original e  $C$  a mensagem codificada;
- > envia a mensagem  $C$ , ao destinatário.

## O receptor da mensagem:

- > determina o inteiro  $M'$  usando a fórmula de decodificação  $M' = C^d \pmod{n}$ ;
- > como  $M' = M$ , recorre ao “alfabeto digital” e obtém a mensagem original.

## Exemplo:

### Determinação das chaves

- > Primos  $p=11$  e  $q = 23$ ;  $n = 11 \times 23 = 253$ , e  $\phi(n) = (11 - 1)(23 - 1) = 10 \times 22 = 220$ .
- > Como  $\text{m.d.c.}(3, 220) = 1$ , o expoente de codificação é  $e = 3$ .
- > Como  $3d = 1 \pmod{220}$  -  $d = 147$ , o expoente de codificação é  $d = 147$ . Assim, a chave pública é  $(253, 3)$  e a chave privada é  $(253, 147)$ .

### Codificação da mensagem SOL

- > Recorrer-se a um “alfabeto digital”:  $M = 191512$ .
- > Como  $M > n = 253$ , divide-se  $M$  em blocos  $M_1 = 19$ ,  $M_2 = 15$  e  $M_3 = 12$ .
- > Usando a chave pública  $(253)$ , efetua-se a codificação de cada um dos blocos:  $19^3 = 6859 = 28 \pmod{253}$ ,  $15^3 = 3375 = 86 \pmod{253}$  e  $12^3 = 1728 = 210 \pmod{253}$
- > A mensagem codificada é  $C = 2886210$ .

### Decodificação da mensagem

- > Usando a chave privada,  $(253, 147)$ , tem-se:  $28147 = 19 \pmod{253}$ ,  $86147 = 15 \pmod{253}$  e  $210147 = 12 \pmod{253}$
- > Portanto,  $M' = 191512 = M$
- > Conhecido o número  $M$ , basta recorrer ao “alfabeto digital” para obtermos a mensagem inicial: SOL.

## Assinatura Digital

Logicamente, nos dias de hoje, cifras tão simples como a Cifra de César, e até mesmo aquelas mais complexas utilizadas antigamente, seriam facilmente quebradas pelo uso de computadores, através de um método denominado “força-bruta”, onde são realizadas tentativas sucessivas até se chegar à chave desejada.

A criptografia moderna, essencial para a segurança de computadores conectados em rede, especialmente à internet, consiste em algoritmos complexos, de forma a dificultar ao máximo a ação de invasores.

As funções de criptografia aplica-

das aos computadores podem ser divididas em duas categorias: *criptografia* e *autenticação*.

## Criptografia

O ato de criptografar, conforme já abordado e detalhado a seguir, se refere ao embaralhamento das informações de uma mensagem, de forma que alguém sem autorização não possa compreendê-la.

## Autenticação

Já a autenticação é o procedimento para verificação de autenticidade do emissor da mensagem. Para realizar uma autenticação, é necessário proteger a mensagem de forma que ela não

seja modificada, o que é normalmente feito através da incorporação de uma *assinatura digital*.

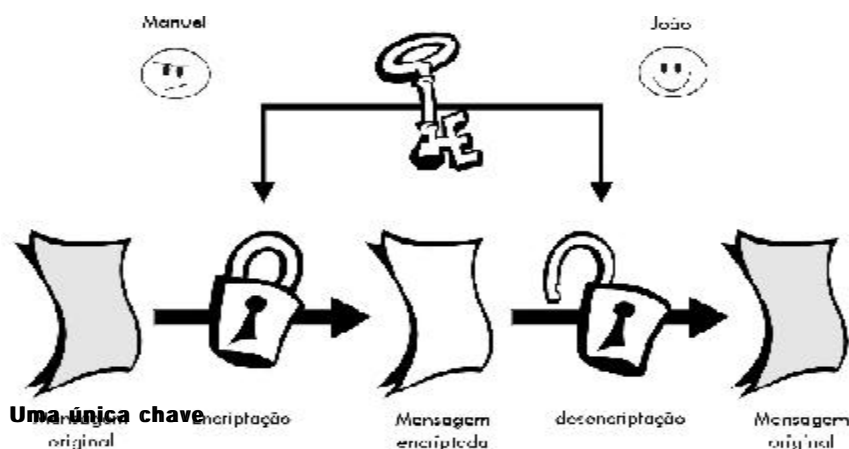
Tipicamente, uma assinatura é formada pela utilização de uma função denominada *hash*, que consiste no cálculo e codificação de um resumo da mensagem completa, formando um código de tamanho fixo que é cifrado e transmitido junto com a mensagem original, garantindo a autenticidade da mensagem.

Podemos dividir as técnicas de criptografia em dois tipos básicos: Criptografia Simétrica ou de Chave Privada, onde uma única chave é utilizada para criptografar e decifrar, e Criptografia Assimétrica ou de Chave Pública, onde é usado um par de chaves

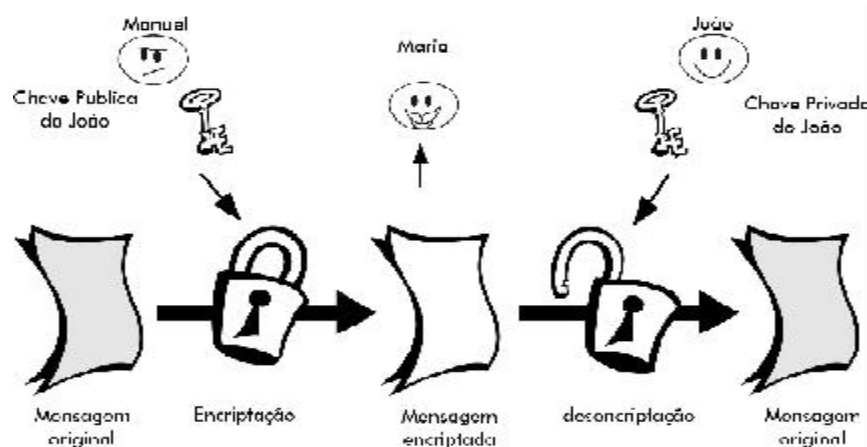
relacionadas entre si, que são a chave pública e a chave privada. As técnicas de criptografia simétricas mais conhecidas são a DES e a AES. O RSA é o algoritmo assimétrico mais conhecido.

## Tipos de Criptografia

### \* Criptografia Assimétrica ou de Chave Pública



### \* Criptografia Simétrica ou de chave secreta



**Duas chaves:** - chave pública, que é publicada;  
- chave privada, que é mantida secreta.

No âmbito da certificação digital, a modalidade mais utilizada é a denominada híbrida, como o protocolo SSL, que utiliza a criptografia assimétrica na inicialização de uma sessão Web, quando é trocada uma chave simétrica, tipo DES, que será utilizada no transcorrer da sessão já iniciada, até o seu término, quando então é descartada.

Tal procedimento visa a alcançar o máximo de segurança - porque a chave simétrica é utilizada apenas uma vez, sendo que ela é gerada dinamicamente, a cada sessão estabelecida - aliado ao mínimo de processamento necessário nos computadores envolvidos. Assim, o algoritmo DES consome menos recursos computacionais quando comparado ao algoritmo RSA utilizado na criptografia assimétrica, ou de chave pública.

Para realizar a assinatura de documentos, é necessária a utilização de um par de chaves, sendo que o emissor assina o documento com sua

chave privada, e o receptor deverá possuir a chave pública do emissor para que possa ser comprovada a autenticidade do documento.

Já no caso de emissão de documento sigiloso criptografado, o procedimento é o oposto, ou seja, o emissor deverá possuir a chave pública do receptor, de forma que somente ele, ao receber o documento, poderá decifrá-lo com a sua chave privada.

No caso de documentos assinados e criptografados, deverão ser seguidos os dois procedimentos anteriormente citados em conjunto.

É importante salientar a diferença entre assinatura digital (explicada acima) e assinatura eletrônica, que pode ser, por exemplo, um e-mail transmitido em claro, o qual não possui garantia de autenticidade.

A geração de um par de chaves está demonstrada no quadro da página ao lado.

## Certificação Digital

A certificação digital é o procedimento que utiliza um arquivo eletrônico que acompanha um documento assinado de forma digital, cujo conteúdo é criptografado. Este documento é denominado *certificado digital* e contém informações que identificam a pessoa e/ou computador com que se está tratando na rede. Um documento eletrônico que possui certificação digital tem garantia de autenticidade de origem e autoria, de integridade de conteúdo, de confidencialidade e de não-repúdio, ou seja, de que a transação, depois de efetuada, não poderá ser negada pela parte que

utilizou a certificação.

O certificado digital é uma credencial eletrônica definida de acordo com o padrão ITU-T X.509, e é emitido por uma Autoridade Certificadora (terceiro de confiança) que garante a identidade do portador / usuário de forma análoga a uma Carteira de Identidade.

A Autoridade Certificadora - AC- e a Autoridade de Registro - AR- são entidades de confiança responsáveis pela emissão dos certificados, bem como pela manutenção de toda a estrutura vinculada à certificação digital dentro de seu âmbito de atuação. Dentro da ICP-Brasil, as ACs e ARs estão credenciadas em uma estrutura hierárquica, que tem uma *Chave Raiz* responsável pela geração das Chaves Secundárias, que por sua vez emitem os certificados de usuários.

As aplicações de certificação digital podem ser divididas em duas categorias que são a certificação pessoal e a certificação de servidores.

#### > Certificação Pessoal

- A certificação pessoal refere-se aos certificados emitidos em nome de uma pessoa natural ou jurídica, de forma a identificá-la inequivocamente, ou seja, a pessoa, ou o representante legal da entidade, associada àquela pessoa jurídica.

Tais certificados são utilizados na assinatura de mensagens eletrônicas, bem como no relacionamento dessas pessoas com os aplicativos que exigem a identificação segura de seus usuários.

#### > Certificação de Servidores

- A certificação de servidores se destina à identificação de serviços ou grupos de serviços associados a uma determinada URL primária, Uniform Resource Locator, que é o identificador mundial de documentos e demais recursos na internet, ou seja, todas as URLs derivadas de um determinado endereço eletrônico de um servidor.

Este mecanismo garante que as informações obtidas se originam verdadeiramente daquele endereço certificado, a exemplo dos bancos e demais aplicações que requerem segurança da informação.

São exemplos bem-sucedidos de utilização de certificação digital no Brasil:

- o e-CPF e o e-CNPJ na Secretaria da Receita Federal, que possibilitam o relacionamento seguro via internet dos contribuintes com a instituição para acesso de informações não disponíveis de forma convencional;

- o processo de tramitação eletrônica de documentos oficiais, que serão publicados no Diário Oficial da União, utilizado pelo Presidente e seus ministros, que possui um sistema que faz o controle do fluxo de forma automática, garantindo segurança, agilidade e eficiência;

- o Sistema de Escrituração Fiscal da Secretaria da Fazenda do Estado de Pernambuco, que obriga que os lançamentos de registro de operações e prestações relativas ao ICMS sejam feitos através de arquivo eletrônico assinado de forma digital, que incorpora uma série de benefícios, tais como: entrega de vários documentos em uma única remessa, redução drástica no volume de

erros de cálculo involuntário, eliminação de múltiplas escriturações, redução de custos de escrituração e armazenamento de livros fiscais, etc.;

- sistema de encaminhamento de Petições Eletrônicas no TRT-4 do Rio Grande do Sul, agilizando o tempo de cada processo de forma segura e econômica;

- o sistema PUBNet da Imprensa Oficial de São Paulo, que automatiza por completo todo o ciclo de publicações na internet de forma segura e rápida, evitando-se congestionamentos telefônicos anteriormente registrados com constância. Também foi possível, através do uso da certificação digital, a criação do e-diário oficial, que é o Diário Oficial em formato eletrônico.

#### Certificação Digital no Estado de Minas Gerais

Recentemente, a administração pública estadual identificou a necessidade de automatizar determinados processos de tramitação de documentos em sua esfera, necessitando, portanto, de ferramentas capazes de, eletronicamente, controlar o fluxo dos documentos com segurança, garantia de autenticidade e autoria, bem como com garantia de sigilo em determinados processos protegidos pela legislação em vigor.

Com base em tais requisitos, optou-se, como não poderia deixar de ser, por tecnologias envolvendo certificados digitais para pessoas físicas e jurídicas, em suas interações com o poder público estadual.

Foram consideradas as possibilidades existentes no mercado

como a criação de uma infra-estrutura de chaves públicas (ICP) estadual, baseada em certificados digitais próprios do Estado, bem como a sua adesão à ICP-Brasil.

Essa adesão foi decidida em função da garantia de validade jurídica nos relacionamentos eletrônicos conforme disposto no texto da Medida Provisória 2.200-2, bem como pelos fatores técnicos de segurança, já que a ICP-Brasil possui regras rígidas para credenciamento, com auditorias regulares, aumentando, dessa forma, a credibilidade dos certificados emitidos.

Avaliando-se as várias alternativas técnico-econômicas apresentadas, optou-se pela adesão do Estado à ICP-Brasil, por intermédio da contratação de uma autoridade certificadora de primeiro nível, ou seja, diretamente subordinada à raiz da ICP-Brasil, que terceirizaria as atividades relacionadas à infra-estrutura de segurança necessária ao desempenho das funções relacionadas à emissão dos certificados, bem como pela guarda da chave primária da AC estadual.

Através da instauração de um grupo de trabalho específico para deliberar sobre o assunto, ficou determinado que seria a Prodemge a Autoridade Certificadora do Estado.

Através de um processo licitatório, a Prodemge contratou a empresa Certisign como a provedora da infra-estrutura necessária. Cumpridas as determinações do ITI, foi publicado o Despacho da entidade, reconhecendo formalmente a Prodemge como Autoridade Certificadora e Autoridade de Registro, dentro dos padrões

da ICP-Brasil.

Várias iniciativas estão em curso no Estado para a utilização de certificados digitais em aplicações do Governo de Minas Gerais, principalmente aquelas que possibilitem a desburocratização dos procedimentos usuais das empresas e cidadãos nos seus relacionamentos com o Estado.

Podemos destacar, entre essas iniciativas, as seguintes:

- tramitação segura de documentos (Workflow) entre os diversos segmentos governamentais, garantindo maior agilidade, segurança e redução de custos pela diminuição da burocracia;

- digitalização / Gestão Eletrônica de Documentos da Junta Comercial do Estado de Minas Gerais, propiciando uma redução expressiva de documentos, aumentando a segurança e reduzindo o tempo de acesso às informações armazenadas;

- registro eletrônico de alterações contratuais via Web na Junta Comercial do Estado de Minas Gerais, aumentando a segurança, reduzindo o tempo de atendimento e a necessidade de deslocamentos ao local;

- relacionamento seguro, através de certificados, da Secretaria da Fazenda do Estado de Minas Gerais com contribuintes de ICMS, possibilitando o envio e consultas de informações de forma segura e identificada;

- relacionamento seguro de fornecedores do Estado, agilizando os processos de compras e aquisições, em especial com a Secretaria de Planejamento e Gestão, responsável por um volume sig-

nificativo de licitações;

- relacionamento seguro dos servidores estaduais com as diversas instituições, em especial com a Secretaria de Estado de Planejamento e Gestão e o Instituto de Previdência Estadual, possibilitando maior agilidade no atendimento, com redução de custos devido a um maior controle;

- identificação segura dos usuários de sistemas corporativos computadorizados, garantindo segurança e transparência nas atividades do Estado;

- comercialização segura de documentos sob responsabilidade da Imprensa Oficial do Estado de Minas Gerais;

- utilização de correio eletrônico com assinatura por todos os servidores estaduais.

As melhorias incorporadas, com a utilização da certificação digital, nos diversos aplicativos existentes ou em desenvolvimento no Estado de Minas Gerais adicionarão celeridade aos diversos processos, bem como trarão ainda maior transparência às ações da administração pública estadual.

Necessária. Cumpridas as determinações do ITI, foi publicado o Despacho da entidade, reconhecendo formalmente a Prodemge como Autoridade Certificadora e Autoridade de Registro, dentro dos padrões da ICP-Brasil.