Um estudo sobre a ICP-Brasil *(versão 1.3)*

Fernando Verissimo[i] Rio de Janeiro, 7 de outubro de 2002.

Hoje assisti à palestra “Assinaturas e Certificados Digitais”, sobre Infra-estrutura de Chaves Públicas do Brasil (ICP-Brasil), apresentado pelo Sr. Sérgio Falcão[1] da Câmara Técnica do Documento Eletrônico do Conselho Nacional de Arquivos (CONARQ) e da Câmara dos Deputados. Ele foi convidado pela Comissão Nacional de Energia Nuclear para fazer uma exposição do assunto aqui no Rio de Janeiro. Aliás, já é a segunda vez que eu assisto uma palestra sobre o mesmo tema apresentado por alguém enviado da Câmara dos Deputados. A outra foi no Simpósio Brasileiro de Redes de Computadores (SBRC2002), realizado pela Sociedade Brasileira de Computação (SBC), em maio de 2002, quando o Sr. Bernardo Lins[2] expôs a ICP-Brasil.

Resolvi escrever esse texto para as pessoas que já têm algum conhecimento sobre o assunto e querem se aprofundar, ou para quem leu o meu texto de janeiro deste ano, chamado “Privacidade, Integridade e Irrevogabilidade”, que pode ser encontrado na *intranet* da Academia Brasileira de Ciências ou no meu site na internet *(ver referência no fim do texto)*.

Para começar, eu gostaria de falar de uma dúvida que um dos espectadores da palestra de hoje teve: O que é uma assinatura digital? Se você pensava que uma assinatura digital é o arquivo com a imagem digitalizada (ou *scanneada*) da nossa verdadeira assinatura manuscrita, apague isso da sua mente imediatamente. Aquela imagem não é uma assinatura digital. Um documento texto que você receba com uma assinatura manuscrita digitalizada não tem nenhum valor. Essa imagem pode ser copiada de um outro lugar e colocada ali sem que nenhum perito no mundo possa identificar a sua procedência, ou seja, é fraudável. Aliás, evite enviar a sua

---

[1] Sergio Falcão, Analista de Sistemas da Câmara dos Deputados email: sergio.falcao@camara.gov.br

[2] Bernardo F. E. Lins, Consultor Legislativo da Câmara dos Deputados , email: bernardo.lins@camara.gov.br

ssinatura manuscrita digitalizada através de um meio tão promíscuo quanto a Internet.

Assinatura Digital

Se você pegar o seu documento em meio digital, o seu arquivo com informações, ou qualquer conjunto de bits que você deseja transmitir para uma outra pessoa, com a sua assinatura digital, e passar ele através de um algoritmo matemático de *hash*[3] que gerará um conjunto de bits, que chamaremos de resumo, e passar esse resumo por um algoritmo de criptografia que terá como *chave* a sua chave privada[4], você terá como resultado a sua assinatura digital.

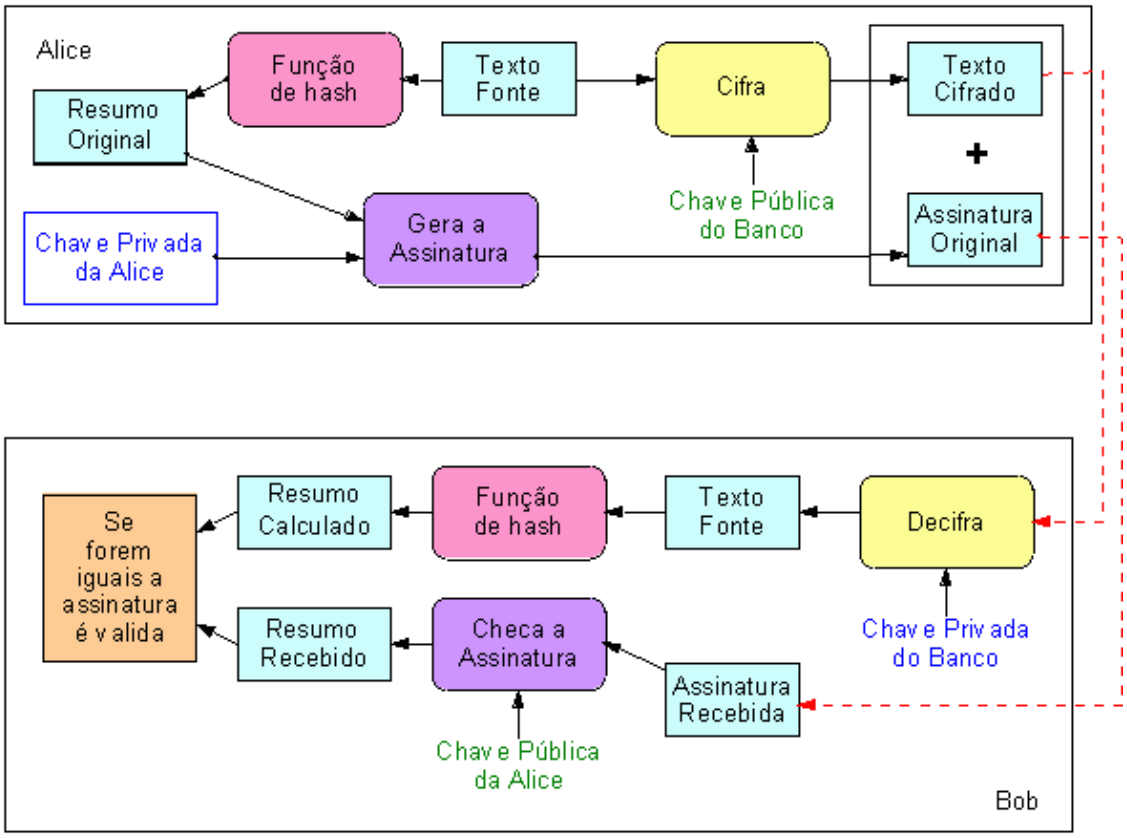

Figura 1

[3] A função hash é uma função que recebe um conjunto de bits que pode ter tamanho variado e devolve um conjunto de bits de tamanho fixo. A função hash garante que dois conjuntos de bits distintos, que sejam recebidos, gerarão dois conjuntos de bits resultado também distintos. Garante também que o mesmo conjunto de bits que entre duas ou mais vezes, sempre gerará o mesmo conjunto de bits resultado. E finalmente, garante que é computacionalmente impossível que, a partir de um conjunto de bits resultado, se encontre o conjunto de bits origem.

[4] Assumi que você já leu a respeito de chaves públicas e chaves privadas no texto "Privacidade, Integridade e Irrevogabilidade".

A figura 1 mostra o processo de assinatura de um documento e da criptografia do mesmo, e depois o processo da decifração e conferência da assinatura.

Como primeira conclusão, temos que a assinatura digital é diferente para cada documento que você vai transmitir.Essa é a assinatura digital que você vai anexar ao documento que você deseja enviar.

A pessoa que recebeu esse documento terá como conferir a sua assinatura digital, pois bastará ela submeter o documento que ela recebeu ao mesmo algoritmo *hash*, e comparar o novo resumo gerado com o resumo que você enviou criptografado, que ela poderá decifrar utilizando a sua chave pública. Os dois resumos, o gerado pela pessoa que recebeu o documento e o que você enviou, têm que ser idênticos, ou ela terá a garantia de que o documento foi alterado durante a transmissão. Caso ela não consiga, utilizando a chave publica de quem enviou o documento, decifrar o resumo enviado, terá garantia de que o documento é falso.

Até agora você deve ter achado o processo muito complicado. Eu omiti um detalhe: O seu único trabalho é imputar a chave privada quando for pedido, todo o processo é feito pelos softwares de comunicação que você já tem instalado no seu computador: MS Internet Explorer, Microsoft Outlook, Qualcomm Eudora, Netscape Communicator, Microsoft Word, etc...

Para que serve a ICP-Brasil

Até agora não disse para que serve a ICP-Brasil. Ela regula um conjunto de entidades governamentais ou de iniciativa privada que serão responsáveis por assegurar que aquele par de chaves, privada e pública, pertence a você. Nós podemos utilizar a tecnologia de assinaturas digitais e criptografia assimétrica, utilizando chaves públicas e privadas sem a necessidade de certificação, mas isso vai depender do caso.

Imagine que eu compre um carro e assine o pedido com a minha chave privada. A concessionária, de posse da minha chave pública que eu forneci, descobre que ela foi realmente assinada por mim, e me envie o carro. Quando a entrega chega à minha porta imediatamente eu sou cobrado pelo veículo.

Então eu informo a ela que não fiz a encomenda. Juridicamente a concessionária não tem como provar que eu criei as chaves e que eu passei a minha chave pública para ela.

Precisamos, então, de uma Autoridade Certificadora (AC), uma espécie de cartório virtual, que garanta que aquele par de chaves está associado a mim, assim como temos um cartório que garante que aquele garrancho que eu fiz no papel é a minha assinatura. Desta forma a concessionária poderia me processar pedindo indenização pelo custo de transporte do veículo que eu agora nego ter pedido.

As utilidades são muitas. Que ver outro exemplo? A maioria de nós entrega declaração de Imposto de Renda pela internet, não é? Você já pensou que nada pode garantir que uma outra pessoa, mal intencionada, faça novamente a sua declaração, alterando violentamente os valores com o intuito de te prejudicar, e envie à Secretaria da Receita Federal dizendo ser uma declaração sua retificadora? De uma hora para outra, você que espera ter uma restituição depois de alguns meses, na verdade estará com uma dívida na SRF, a qual você nem foi notificado.

Os bancos e as administradoras de cartão de crédito então interessadíssimas nisso. Hoje, se você faz uma compra via internet, e depois alega que não comprou, a Administradora se vê obrigada a ficar com o prejuízo sem reclamar.

Isso já é realidade

A novidade é que isso já é realidade há alguns meses, e você não terá como fugir desse avanço. Assim como registrar uma firma num cartório de notas, o registro de suas chaves a unidade certificadora também será um serviço pago. Os preços[5] hoje estão por volta dos R$ 45,00 anuais, ainda caros para o uso popular, mas a concorrência fará esse preço cair para perto de R$ 15,00. Também temos que ter em mente que nem todos precisaremos ter um certificado digital, assim como nem todos temos registro no cartório de notas.

[5] Preço de cessão de chaves para assinatura de email. Existem preços para chaves com vários fins.

Estrutura da ICP-Brasil

A estrutura da ICP-Brasil é mostrada na figura a seguir. Ela possui uma, e só uma, Autoridade Certificadora Raiz (AC-Raiz), que é representada pelo Instituto Nacional de Tecnologia da Informação (ITI). O certificado do ITI é o único que é auto assinado, ele é chamado de certificado raiz. Ninguém garante que o certificado raiz é verdadeiro, isso é garantido pelo órgão máximo da ICP-Brasil, temos que aceitar e confiar. As demais Autoridades Certificadoras possuem os seus certificados garantidos pela AC-Raiz. A AC-Raiz não vende certificados para pessoas e instituições, apenas para Autoridades Certificadoras e é responsável por certificar-se que a Entidade é preparada para ser uma AC, e por auditar o processo. Para se ter uma idéia de como é difícil ser uma AC, o custo para se candidatar a um credenciamento é de R$ 500 mil, e os requisitos técnicos são semelhantes a um filme de ficção científica: caixas fortes à prova de intrusos, choque e fogo, onde ficam os servidores, links de redes com bandas astronômicas, funcionários extremamente especializados e que permitam que suas vidas pessoais sejam investigadas, e por aí vai.

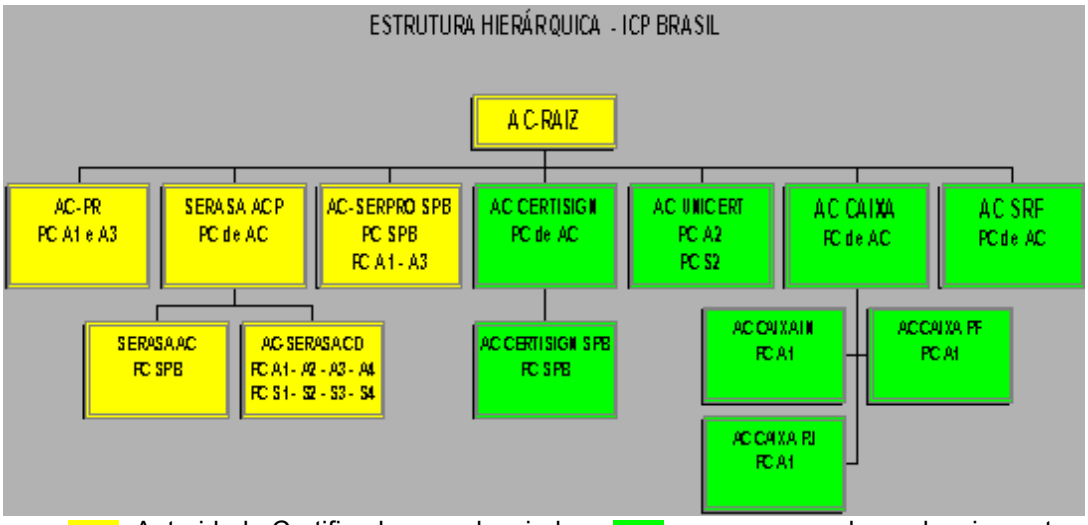

Figura 2 - Posição em 27 de agosto de 2002. Fonte: http://www.iti.gov.br/

O Brasil na frente

Como no caso das eleições e entrega de imposto de renda, o Brasil é um dos pioneiros na adoção dessa nova tecnologia. Os brasileiros, ontem, votaram eletronicamente, enquanto os norte-americanos tiveram enormes

problemas com suas cédulas perfuradas, no ano passado. ICP é novidade no mundo, mas logo isso será comum em todo mundo.

> *O Globo On Line*
> *Data: Segunda-feira, 16 de setembro de 2002*
>
> ***Governo e Microsoft: convênio de assinaturas digitais***
>
> *BRASÍLIA – O ministro-chefe da Casa Civil da Presidência da República, Pedro Parente, assinou há pouco com o gerente-geral da Microsoft do Brasil, Emílo Umeoka, convênio que vai garantir, a partir da primeira semana de outubro, a autenticidade e a legalidade das assinaturas digitais firmadas no Brasil.*
>
> *Pelo convênio, quaisquer assinaturas de pessoas físicas e jurídicas de Direito Público ou Privado terão reconhecimento assegurado pelos sistemas operacionais da Microsoft em todo o mundo. Antes do Brasil, apenas a Suíça e a Irlanda tinham convênios parecidos com o firmado hoje, mas o acordo brasileiro é mais abrangente, pois vale para todos o produtos da Microsoft e não apenas para o Internet Explorer.*
>
> *Agência Brasil*

O governo brasileiro convidou todas as empresas de software para assumirem um contrato de divulgação do certificado raiz do Brasil[6], ou seja, o certificado da AC-Raiz, que é auto-assinado. A Microsoft prontamente respondeu o convite, e já vai distribuir em **todos** os seus produtos esse certificado brasileiro, para **todos** os países do mundo. Isso facilitará que documentos brasileiros sejam reconhecidos em outros países, à medida que as ACs-Raízes desses outros países desejem firmar contratos bilaterais com o Brasil (provavelmente esses acordos já serão firmados eletronicamente).

--X--

ICP-Brasil. http://www.icpbrasil.gov.br. Visitado em 07/10/2002.

MARTINI, Renato. *Criptografia e cidadania digital*. Rio de Janeiro: Editora Ciência Moderna Ltda. 2001.

MARTINS, Alesandro. *Sistema de Certificação e Autenticação*. Seminário de Tópicos Especiais em Redes Integradas Faixa Larga (COS 871). 2000. http://www.ravel.ufrj.br/~verissimo/. Visitado em 16/01/2002.

[6] Informação dada pelo Sr. Luis Roberto Varreto (varreto@planalto.gov.br), membro da Comissão Técnica Executiva da ICP-Brasil e Diretor de TI da Presidência da República.

TERADA, Routo. *Segurança de Dados: Criptografia em Redes de Computadores*. São Paulo: Edgard Blücher. 2000

VERISSIMO, Fernando. Privacidade, Integridade e Irrevogabilidade. 2002. http://www.ravel.ufrj.br/~verissimo/producao.html. Visitado em 07/10/2002.

VERISSIMO, Fernando. Segurança em Redes sem Fio. Seminário de Tópicos Especiais em Redes Integradas Faixa Larga (COS 871). 2001. http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos_academicos.php. Visitado em 16/01/2002.

[i] Fernando Verissimo é Analista de Sistemas da Academia Brasileira de Ciências e mestrando da linha de Redes de Computadores da COPPE/UFRJ. Email: verissimo@pobox.com

Agradeço a colaboração do Alessandro Martins (martins@ravel.ufrj.br) e da Débora Verissimo (iocken@pobox.com) na revisão desse documento.