

A chave da assinatura digital

Fotos Antoninho Perri

LUIZ SUGIMOTO

sugimoto@reitoria.unicamp.br

Em pouco tempo, docentes, funcionários e alunos da Unicamp poderão trocar, via computador, documentos ou mensagens cuja autenticidade será atestada por um certificado digital com o mesmo valor da assinatura em papel. “A adoção deste mecanismo é uma forte tendência no mundo inteiro, já que a tecnologia da informação está permeando todas as áreas de governo e de negócios”, afirma o professor Marco Aurélio Amaral Henriques, que coordena o projeto piloto em andamento no Centro de Computação (CCUEC).

Henriques informa que o governo já criou em 2001 a Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), no âmbito do Instituto de Tecnologia da Informação (ITI). “Hoje em dia, qualquer cidadão pode assinar digitalmente a sua declaração de imposto de renda, embora não seja obrigatório. Para isso, ele deve adquirir o certificado digital – é como se fosse ao cartório e registrasse sua firma. Esta alternativa ainda não está amplamente disseminada devido ao custo, que começa em torno dos cem reais por ano”.

Segundo o coordenador do projeto na Unicamp, o ITI mantém a chamada Autoridade Certificadora Raiz Brasileira, encarregada de credenciar autoridades certificadoras em segundo nível, que cumprem exigências rígidas, inclusive em relação à preservação e guarda dos computadores e ao controle de acesso. “Nada pode acontecer de anormal ou suspeito quando se trata de uma cadeia de confiança. Várias empresas públicas e privadas já foram credenciadas como autoridades certificadoras, como a Secretaria da Receita Federal, Imprensa Oficial do Estado de São Paulo e Caixa Econômica Federal”.

São estas instituições que a população e as empresas devem procurar para obter o certificado digital, que possui valor legal, como ressalta Henriques. “Em abril de 2007, a então presidente do Supremo Tribunal Federal, ministra Ellen Gracie, elaborou a primeira decisão em um processo formal usando certificação digital. Ainda falta muito para fazer todo o trâmite dos processos de forma totalmente digital, sem suporte em papel, mas já existe a tecnologia para isso”.

Criptografia

Marco Aurélio Henriques, que é superintendente do CCUEC e docente da Faculdade de Engenharia Elétrica e de Computação (FEEC), explica que a assinatura digital, na verdade, é uma sequência de bits anexada ao final do documento para garantir sua autenticidade e integridade. “Alguns recibos de banco trazem uma sequência de números e letras depois do histórico das operações efetivadas. Trata-se de uma espécie de assinatura digital, pois é criada por meio de uma chave (senha) que só o banco conhece”.

O pesquisador esclarece que em criptografia todo documento – texto, foto, vídeo – é visto como uma sequência de números, recorrendo-se comumente a um algoritmo para realizar operações matemáticas complexas que cifram os dados originais de maneira a torná-los ininteligíveis. “Se quero enviar uma mensagem sigilosa, passo o arquivo por um algoritmo de criptografia (existem vários disponíveis) e uso



O professor Marco Aurélio Amaral Henriques, coordenador de projeto piloto no CCUEC: “Nada pode acontecer de anormal ou suspeito quando se trata de uma cadeia de confiança”

uma chave. Mesmo os computadores mais velozes do mundo, trabalhando em conjunto, levariam milhares de anos para descobrir a chave”.

Na criptografia clássica, que reinou soberana até pouco mais de 30 anos atrás, remetente e destinatário precisam conhecer a mesma chave para cifrar e decifrar uma mensagem, o que remete à história de Alice, Bob e da espiã Eva que ilustra os livros. “Este compartilhamento de uma chave única é um problema, pois Alice e Bob, para trocar mensagens secretas, têm que se encontrar em algum momento para combinar a chave, ou correr o risco de que ela seja interceptada pela espiã Eva caso recorram a algum outro meio de comunicação para isso”.

Chave pública

De acordo com Henriques, houve

uma revolução na área de criptografia em 1976, quando se passou a construir, com novos algoritmos, um par de chaves irmãs: uma privada, que permanece sigilosa para sempre, e outra pública, que pode ser divulgada amplamente. “Tenho uma página na Web com minha chave pública. É um número gigantesco, que toda pessoa pode usar com um algoritmo apropriado para cifrar uma mensagem que queira me enviar. A única forma de decodificá-la é com a minha chave privada, que só eu conheço, o que dá ao remetente a certeza de sigilo”.

Já a assinatura digital, reitera o professor, serve para atestar a origem e o autor de uma mensagem enviada, mediante processo inverso. “O que se faz é aplicar à mensagem um programa de codificação, utilizando a chave privada. Do outro lado, o texto poderá ser

decodificado por qualquer pessoa com acesso à chave pública correspondente. Se a operação é bem sucedida, tem-se a certeza de quem foi o responsável pela mensagem. É a codificação com uma chave privada que caracteriza uma assinatura digital”.

Entretanto, Marco Aurélio Henriques atenta para a necessidade de uma medida de segurança fundamental. “A questão é se certificar que a chave pública divulgada em uma página da Web ou num cartão de visitas é mesmo de determinada pessoa. Um impostor poderia assinar um documento com a sua chave privada e divulgar a chave pública como sendo de outra pessoa, fazendo crer a todos que fosse dela a assinatura”.

Certificação

É para certificar esta assinatura, ob-

Professor da FEEC coordena projeto que prevê a adoção de mecanismo que ganha espaço em todo o mundo

serva o pesquisador, que foi montada a Infra-Estrutura de Chaves Públicas do governo brasileiro, que funciona como um sistema de cartório digital. “Usando o próprio computador, a pessoa interessada pode criar seu par de chaves privada e pública. Juntando-se uma série de documentos convencionais que garantam a identidade do usuário, a chave pública deve ser registrada em uma autoridade certificadora credenciada pela ICP-Brasil”.

Henriques acrescenta que o interessado receberá um certificado atestando ser ele o portador da chave pública. Este documento será assinado digitalmente com a chave privada da autoridade, que entregará ao usuário sua própria chave pública, também na forma de um certificado digital assinado pela Autoridade Certificadora Raiz. “O que a pessoa torna público é seu certificado digital e não apenas a sua chave pública. Assim, outros que também registraram suas senhas e receberam a chave pública da autoridade, têm como verificar a autenticidade dos certificados uns dos outros”.

Conforme Marco Aurélio Henriques, o que está sendo construído na Unicamp é uma autoridade certificadora. “Por enquanto, os certificados que emitirmos não terão o mesmo valor legal que aqueles da ICP-Brasil, mas eles poderão ser de grande utilidade na validação de documentos e mensagens trocados no âmbito da universidade e entre ela e as demais instituições brasileiras que estão iniciando projetos similares”.

SERVIÇO

Para mais informações sobre o projeto piloto em curso no CCUEC: www.ccuec.unicamp.br/icp

Para o uso acadêmico

No contexto da Unicamp, o professor Marco Aurélio Henriques observa que a assinatura digital poderia autenticar, por exemplo, boletins de notas e frequências enviados pelos professores à Diretoria Acadêmica ou oficiais relacionados à movimentação de convênios junto à Funcamp. Da mesma forma, a DAC teria uma nova ferramenta para certificar atestados de matrícula ou históricos escolares solicitados por alunos que pleiteiam vagas em empresas.

É com este propósito que a Unicamp vem participando do projeto Infra-Estrutura de Chaves Públicas Educacional (ICP-Edu), iniciado pela Rede Nacional de Ensino e Pesquisa (RNP) do Ministério da Ciência e Tecnologia. “A idéia é promover o trâmite de documentos assinados digitalmente entre universidades, além de abrir um campo para pesquisas, testes e familiarização

da comunidade com estas tecnologias e ferramentas”.

Segundo Henriques, o projeto, que está sendo expandido para várias outras instituições brasileiras, envolve seis nesta fase inicial: Laboratório Nacional de Computação Científica, a própria RNP e as universidades federais de Minas Gerais, Santa Catarina e Fluminense, sendo a Unicamp a única universidade estadual. “Estamos nesta fase do projeto graças aos esforços do professor Ricardo Dahab, do Instituto de Computação, pesquisador muito ativo e conhecido na área”.

A RNP criou a Autoridade Certificadora Raiz da ICP-Edu e todas as demais instituições já criaram suas autoridades certificadoras de segundo nível. Ainda em caráter experimental, foi criada a AC Unicamp e iniciado um projeto piloto dentro do Centro de Computação, com a participação

dos seus funcionários. “Estão sendo emitidos certificados que, por enquanto, servem apenas para assinar mensagens eletrônicas. Também é possível enviar uma mensagem sigilosa, codificando-a com a chave pública do destinatário, a fim de que somente ele consiga decodificá-la”.

No âmbito do projeto da Rede Nacional de Ensino e Pesquisa, o Centro de Computação da Unicamp pode enviar documentos assinados digitalmente para qualquer uma das universidades participantes. “É importante destacar que estes documentos, embora certificados pela ICP-Edu, não possuem valor legal fora das instituições. Mas o sistema serve muito bem para a troca de documentos autenticados digitalmente entre universidades ou entre órgãos da Unicamp”.

Marco Aurélio Henriques adianta que, para expandir a assinatura digital ao restante da Uni-

camp, será preciso estabelecer novas formas de trabalho com órgãos que emitem identidades, como a Diretoria Geral de Recursos Humanos (DGRH), responsável pela identidade funcional dos docentes e funcionários contratados, e a Diretoria Acadêmica (DAC), que fornece o cartão universitário aos estudantes.

Uma proposta é que a própria identidade funcional já contenha o certificado digital. “A Unicamp já tem o privilégio de fornecer à sua comunidade o chamado *smart card*, cartão inteligente que é munido do chip capaz de guardar de forma inviolável a chave privada do usuário. O aproveitamento deste cartão vem sendo objeto de estudos e avaliações com o patrocínio do banco Santander. São muito animadoras as perspectivas para sua adoção no cotidiano da Universidade”.