Assinatura eletrônica baseada em certificação digital – Parte IV

Um certificado, elemento caracterizador da assinatura eletrônica na modalidade digital, é um arquivo eletrônico que contém uma série de informações específicas, tais como: a) a chave criptográfica pública do usuário; b) o nome do usuário; c) o número de série e d) o prazo de validade do certificado. O certificado digital é um arquivo assinado pela entidade responsável pela geração do par de chaves criptográficas (autoridade certificadora – AC ou *certificate authority* - CA).

A autoridade certificadora – AC funciona praticamente como um "cartório eletrônico". Ela atesta ou garante, por intermédio de sua assinatura no certificado, que a chave pública nele presente foi efetivamente gerada como um dos elementos do par de chaves criptográficas de um determinado usuário (com nome registrado no próprio certificado).

A chave pública da autoridade certificadora, usada para assinar o certificado do usuário, integra uma infra-estrutura de chaves públicas. Essa infra-estrutura hierarquizada de chaves públicas remete a uma chave inicial (chave-raiz). A chave inicial (chave-raiz) é auto-assinada (o certificado é assinado com a própria chave privada do par). Registre-se a possibilidade de um modelo não-hierárquico (como uma rede de chaves públicas individuais interconectadas).

A chamada Infra-Estrutura de Chaves Públicas - ICP (ou *Public Key Infraestructure - PKI*) envolve o conjunto das autoridades certificadoras, as políticas de certificação e os protolocos técnicos utilizados na certificação digital. Atualmente, no Brasil, existe uma ICP oficial (a ICP-Brasil), regulada pela Medida Provisória n. 2.200-2, de 2001. Veja a estrutura da ICP-Brasil e outras informações importantes sobre certificação digital no seguinte endereço eletrônico: **http://www.iti.gov.br**. Trata-se do *site* do Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal que funciona

como a Autoridade Certificadora Raiz da ICP-Brasil.

O uso de certificados digitais afasta os golpes envolvendo *sites* falsos na internet. Um *site* pode ser copiado. O endereço eletrônico pode ser confundido pela extrema semelhança com o verdadeiro. A aparência (os elementos visuais) pode ser reproduzida nos mínimos detalhes. Entretanto, o certificado digital vinculado ao *site* não pode ser apresentado pelo falsário.

Na situação acima sugerida, o navegador (*browser*) do usuário contém uma lista de autoridades certificadoras confiáveis. Assim, quando o usuário acessa um *site* e recebe o pertinente certificado digital, o navegador verifica se a autoridade certificadora que o expediu integra a lista de confiáveis. Quando a autoridade certificadora não integra a lista aludida, o usuário é chamado a escolher entre confiar permanentemente, temporariamente ou não confiar na entidade geradora do certificado.

O certificado digital, tal como explicado anteriormente, resolve uma das fragilidades do chamado “documento eletrônico puro e simples” (aquele simplesmente confeccionado como documento eletrônico). Com a certificação digital (a rigor, com a intervenção da autoridade certificadora) resta solucionado o problema da autenticidade do documento eletrônico.

É possível, com a utilização do certificado digital, afirmar quem é o autor do documento eletrônico sobre o qual foi aplicada uma chave privada. Com efeito, a chave pública de A, presente no certificado digital “garantido” pela autoridade certificadora, somente decodifica o arquivo criptografado pela chave privada de A.

Brasília, 4 de março de 2007.

Aldemario Araujo Castro

Mestre em Direito

Professor de Informática Jurídica e Direito da Informática da Universidade Católica de Brasília

Coordenador da Especialização (a distância) em Direito do Estado da Universidade Católica de Brasília

Procurador da Fazenda Nacional

Membro do Conselho Consultivo da Associação Paulista de Estudos Tributários – APET

Co-autor do livro Manual de Informática Jurídica e Direito da Informática

Site: http://www.aldemario.adv.br