Assinatura eletrônica baseada em certificação digital – Parte III

Como foi registrado anteriormente, a superação da fragilidade ou insegurança da criptografia *simétrica* (de chave única) ocorreu com o desenvolvimento da criptografia *assimétrica* (com duas chaves distintas e relacionadas entre si - um par de chaves).

Na criptografia assimétrica, uma das chaves é chamada de *pública* e a outra de *privada*. A primeira, como a denominação sugere, pode ser de conhecimento geral. Já a segunda, na linha de sua nomenclatura, deve ser mantida em segredo (conhecida somente pelo seu proprietário ou usuário).

O funcionamento da criptografia assimétrica pressupõe: a) que o texto codificado por uma das chaves do par somente será decodificado pela outra chave e b) a inviabilidade da descoberta da chave privada a partir da chave pública (admitindo um tamanho considerável para as chaves envolvidas).

direito	chave ========> privada de A	**6Tf9*qD23**	chave ========> pública de A	**direito**
direito	chave ========> pública de A	**Mn86%Yy6**	chave ========> privada de A	**direito**

Observe que as chamadas “conexões seguras” na internet valem-se, em regra, do par de chaves criptográficas. Assim, o usuário de determinado *site*, quando precisa transmitir informações críticas (dados pessoais, números de cartão de crédito, senhas, etc), recebe uma chave pública (de um par de chaves) em seu computador (situação em que o

navegador exibe um ícone de segurança, a exemplo do famoso “cadeado amarelo”). A partir daí, todas as informações enviadas pela Grande Rede são antes criptografadas com a chave (pública) recebida. Durante o tráfego, até o computador do *site* de destino, os dados são completamente incompreensíveis. Ao chegarem no destino, os dados serão decodificados com a chave privada (o outro elemento do par), único meio de recuperar a informação original e compreensível.

O ícone de segurança no navegador (o “cadeado amarelo”, por exemplo) indica a presença de uma chave criptográfica no computador do usuário (convém verificar se o navegador “fechou” o cadeado). Ao clicar no ícone de segurança é possível visualizar um arquivo (certificado) que contém, entre outras informações, a chave criptográfica transmitida para o computador do usuário.

Portanto, o certificado digital (contendo uma chave pública) é o elemento que permite vincular ou associar determina pessoa a sua chave pública e, por conseqüência, a chave privada correspondente (na medida em que a chave pública consegue desfazer as operações realizadas pela chave privada).

Brasília, 25 de fevereiro 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