Assinatura eletrônica baseada em certificação digital – Parte V

Como já foi registrado anteriormente, a assinatura digital, modalidade de assinatura eletrônica, consegue garantir, em relação aos arquivos eletrônicos (particularmente, os documentos eletrônicos), autenticidade (identificação do autor), integridade (verificação de ausência de modificações no conteúdo) e privacidade (ocultação do conteúdo).

A forma mais “simples” de assinatura digital é aquela realizada tão-somente com o conteúdo da própria mensagem. Nesse caso, o processo envolve os seguintes passos: a) a mensagem é codificada com a chave privada do usuário; b) são enviados para o destinatário os seguintes elementos: b.1) a mensagem original; b.2) a mensagem codificada com a chave privada e b.3) a chave pública do usuário; c) o destinatário decodifica a mensagem cifrada com a chave pública e d) o destinatário compara a mensagem decifrada com a mensagem original. Se a mensagem decodificada for igual a mensagem original temos a indicação de ausência de alterações. Por outro lado, a desigualdade entre os elementos aludidos aponta para a ocorrência de modificações no teor da mensagem depois da aplicação da chave privada.

A sistemática descrita no parágrafo anterior suscita alguns problemas significativos. As principais dificuldades estão relacionadas com o tempo de envio e processamento e as mensagens com conteúdo original “estranho”. Observe-se a necessidade de cifrar e decifrar todo o conteúdo da mensagem, independentemente de sua extensão. Deve ainda ser considerado que o conjunto transmitido possui o dobro do tamanho (da mensagem original). Ademais, as mensagens originais de conteúdo incomum (série de números aleatórios, coordenadas, etc) geram uma considerável insegurança no destinatário quanto à sua regularidade.

A introdução das chamadas *funções hash* no processo de assinatura digital supera as dificuldades mencionadas. As funções

hash, como “algoritmos de resumo”, dispensam a codificação e a transmissão de toda a mensagem original.

A assinatura digital “com hash” funciona de forma distinta da assinatura digital “sem hash”, descrita anteriormente de maneira simplificada. Nesse caso, o processo envolve: a) a aplicação de um algoritmo hash sobre a mensagem original e a obtenção de um resumo do conteúdo do texto conhecido como *message digest (*com tamanho em torno de 128 *bits*); b) a aplicação da chave privada do usuário ao *message digest* e a obtenção do *message digest* criptografado ou codificado; c) envio ao destinatário dos seguintes elementos: c.1) mensagem original; c.2) *message digest* codificado e c.3) chave pública do usuário; d) no destino, o *message digest* será decodificado com a chave pública do remetente; e) também no destino, sobre a mensagem original será aplicado o mesmo algoritmo hash utilizado na origem; f) o *message digest* decodificado será comparado com aquele gerado a partir da mensagem original. A coincidência entre o *message digest* recebido e decodificado e o *message digest* gerado indica que o texto não foi alterado, portanto mantém-se íntegro. A discrepância indica a alteração do documento depois de assinado digitalmente.

O sistema de criptografia assimétrica permite o envio de mensagens com total privacidade. Para tanto, o remetente deve codificar o texto utilizando a chave pública do destinatário. Depois, o remetente deverá criptografar o texto resultante da primeira operação com a sua chave privada. O destinatário, ao receber a mensagem, irá decifrá-la, primeiro, utilizando a chave pública do remetente. O passo seguinte será aplicar a própria chave privada para ter acesso ao conteúdo original da mensagem.

Brasília, 11 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