O que é Certificação Digital ?

Os computadores e a Internet são largamente utilizados para o processamento de dados e para a troca de mensagens e documentos entre cidadãos, governo e empresas. No entanto, estas transações eletrônicas necessitam da adoção de mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas. A certificação digital é a tecnologia que provê estes mecanismos.

Quais são os Benefícios ?

Com a certificação digital é possível utilizar a Internet como meio de comunicação alternativo para a disponibilização de diversos serviços com uma maior agilidade, facilidade de acesso e substancial redução de custos.

O que é Criptografia ?

A palavra criptografia tem origem grega e significa a “arte de escrever em códigos” de forma a esconder a informação na forma de um texto incompreensível, chamado de cifrado.

A tecnologia da certificação digital foi desenvolvida graças aos avanços da criptografia nos últimos 30 anos, sendo que, os processos de cifragem e decifragem são realizadas por programas de computador.

Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número chave que é utilizado para definir como o programa irá se comportar, sendo que, sem o conhecimento da chave correta não é possível decifrar um dado texto cifrado. Assim, para manter uma informação secreta, basta cifrar a informação e manter em sigilo a chave.

E o que é Chave Pública e Chave Privada ?

Atualmente existem dois tipos de criptografia: a simétrica e a de chave pública. A criptografia simétrica realiza a cifragem e a decifragem de uma informação através de algoritmos que utilizam a mesma chave, garantindo sigilo na transmissão e armazenamento de dados. Como a mesma chave deve ser utilizada na cifragem e na decifragem, a chave deve ser compartilhada entre quem cifra e quem decifra os dados, sendo que, a troca de chaves deve ser feita de forma segura, uma vez que todos que a conhecem podem decifrar a informação ou mesmo reproduzi-la.

Os algoritmos de chave pública operam com duas chaves distintas: chave privada e chave pública. Essas chaves são geradas simultaneamente e são relacionadas entre si, o que possibilita que a operação executada por uma seja revertida pela outra. A chave privada deve ser mantida em sigilo e protegida por quem gerou as chaves. A chave pública é disponibilizada e tornada acessível a qualquer indivíduo que deseje se comunicar com o proprietário da chave privada correspondente, permitindo garantir tanto a

confidencialidade quanto a autenticidade das informações por eles protegidas.

E o que é Assinatura Digital ?

A mesma metodologia de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função resumo, também conhecido como função de “hash”, é chamada de assinatura digital.

O resultado deste processo pode ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente.

Em agosto de 2001, a Medida Provisória 2.200 garantiu a validade jurídica de documentos eletrônicos e a utilização de certificados digitais para atribuir autenticidade e integridade aos documentos. Este fato tornou a assinatura digital um instrumento válido juridicamente.

E como é a autenticação disto ?

Para autenticar uma assinatura digital é necessário inicialmente realizar duas operações: calcular o resumo criptográfico do documento e decifrar a assinatura com a chave pública do signatário. Se forem iguais, a assinatura está correta, o que significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está íntegro.

Porque confiar em um Certificado Digital ?

Entre os campos obrigatórios do certificado digital encontra-se a identificação e a assinatura da entidade que o emitiu, os quais permitem verificar a autenticidade e a integridade do certificado. A entidade emissora é chamada de Autoridade Certificadora ou simplesmente AC, que é o principal componente de uma Infra-Estrutura de Chaves Públicas e é responsável pela emissão dos certificados digitais.

Para a emissão dos certificados, as ACs possuem deveres e obrigações que são descritos em um documento público chamado de Declaração de Práticas de Certificação – DPC.

No Brasil, o Comitê Gestor da ICP-Brasil é o órgão governamental que especifica os procedimentos que devem ser adotados pelas Acs, tendo o cumprimento dos procedimentos auditado e fiscalizado, envolvendo, por exemplo, exame de documentos, de instalações técnicas e dos sistemas envolvidos no serviço de certificação, bem como seu próprio pessoal. Sendo que, as ACs credenciadas são incorporadas à estrutura hierárquica da ICP-Brasil e representam a garantia de atendimento dos critérios estabelecidos em prol da segurança de suas chaves privadas.

E quais são as responsabilidades ?

A certificação digital traz diversas facilidades, porém seu uso não torna as transações realizadas isenta de responsabilidades. Ao mesmo tempo que o uso da chave privada autentica uma transação ou um documento, ela confere o atributo de não-repúdio à operação, ou seja, o usuário não pode negar posteriormente a realização daquela transação. Por isto, é importante que o usuário tenha condições de proteger de forma adequada a sua chave privada.

Existem dispositivos que incrementam a proteção das chaves, como os cartões inteligentes (smart cards), semelhantes em formato e tamanho a um cartão de rédito convencional. Os smart cards são um

tipo de hardware criptográfico dotado de um microchip com memória capaz de armazenar e processar diversos tipos de informações. Com eles é possível gerar as chaves e mantê-las dentro de um ambiente seguro, uma vez que as operações criptográficas podem ser realizadas dentro do próprio dispositivo.

Outra alternativa é manter as chaves privadas no próprio computador, porém, neste caso, são necessárias algumas medidas preventivas para minimizar a possibilidade de se comprometer sua sigilosidade ou integridade.

Em caso de suspeita de comprometimento da chave privada, seja por uma invasão sofrida no computador ou pelo surgimento de operações associadas ao uso da chave que não sejam de conhecimento do seu proprietário, a revogação do certificado deve ser solicitada o mais rapidamente possível à AC responsável pela sua emissão.

E qual é a Validade ?

O certificado digital, diferentemente dos documentos utilizados usualmente para identificação pessoal como CPF e RG, possui um período de validade, sendo que, a cada renovação da validade, renova-se também a relação de confiança entre seu titular e a AC. Só é possível assinar um documento enquanto o certificado é válido, sendo possível, no entanto, conferir as assinaturas realizadas mesmo após o certificado expirar.

Por solicitação de seu titular encaminhada à AC, o certificado digital pode ser revogado antes do período definido para expirar. As justificativas podem ser por diversos fatores como comprometimento da chave privada, alterações de dados do certificado ou qualquer outro motivo.

A renovação do certificado pode ser necessária para a substituição da chave privada por uma outra tecnologicamente mais avançada, tendo como objetivo tornar mais robusta a segurança em relação às técnicas de autenticação e às informações contidas no certificado.

Régis E. S. Aguiar. Diretor do IARGS – Office Center, Consultor Sênior Associado da e-trust, Administrador de Empresas e Contador, Auditor Líder ISO27001 e ISO9000, atuou como gestor da segurança da informação na primeira certificação na norma ISO27001 no ramo metal-mecânico no Brasil.