

Segurança da Informação

Certificação e Assinatura Digital

José Maurício S. Pinheiro

UniFOA - 2008

Certificado Digital

- Versão digital de um documento de identidade. É usado como forma de identificação, por mostrar a chave privada (pertencente à autoridade certificadora) que se relaciona com uma chave pública.
- Também chamado de “Certificado de Chave Pública” - produz a garantia que a chave pública pertence à entidade de origem e que ela (e somente ela) possui a chave privada correspondente.

Certificado Digital

- Contém os dados de identificação da pessoa ou instituição que deseja comprovar, perante terceiros, a sua própria identidade. Serve, igualmente, para conferir a identidade de terceiros.
- A validação do certificado passa pela verificação das informações do certificado e, depois, pela assinatura digital da autoridade certificadora.

Certificado Digital

- Ligação entre a chave pública de uma entidade e um ou mais atributos relacionados a esta entidade, armazenados em arquivo digital.
- O usuário pode ser uma pessoa, dispositivo de hardware ou um processo de software.
- Pode ser usado como assinatura em e-mail, controle de acesso a recursos, autenticidade de programas na Internet, etc.

Certificado Digital

- Alternativa para substituir a autenticação por *login* e senha e permite aumentar o nível de segurança em sistemas computacionais.
- Os certificados são emitidos e mantidos por uma autoridade certificadora que funciona como uma espécie de cartório digital. Esta autoridade pode ser representada por uma entidade externa de confiança ou pela própria organização quando a aplicação em questão for restrita à corporação.

Autoridade Certificadora

- Autoridade Certificadora (CA) - entidade responsável por garantir a validade de um certificado digital.
- Aceita aplicações certificadas de certa entidade, autentica aplicações, emite certificados e mantém atualizadas as informações sobre os certificados digitais emitidos.

Autoridade Certificadora

- Autoridades Certificadoras podem ser públicas (cidadãos em geral) ou corporativas (empresas).
- ICP - Brasil (Infra-estrutura de Chaves Públicas Brasileira) - atende aos cidadãos por meio de Autoridades Certificadoras (CA's) e Autoridades de Registro (RA's).

Geração e Transferência de Chaves

- O usuário gera o par de chaves localmente, armazena a chave privada e envia a chave pública para registro na CA.
- *Smart Cards* são usados para gerar o par de chaves utilizando criptografia. A chave pública é divulgada e a chave privada armazenada no cartão.

Geração e Transferência das Chaves



Padrão X.509 v3

Nº da versão X509 do certificado (1, 2 ou 3)

Identificador único do certificado e representado por um inteiro

Identificador do algoritmo usado para assinatura do certificado pela CA

Nome da CA que produziu e assinou o certificado

Tempo que determina a validade do certificado para as aplicações

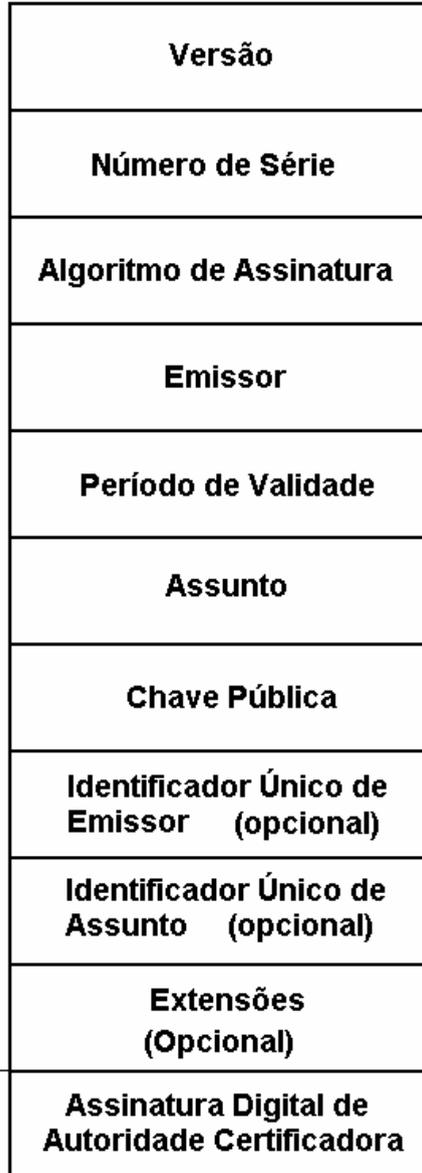
Identifica de forma única o dono da chave pública do certificado emitido pela CA

Contém o valor da chave pública do certificado e informações do algoritmo

Permite o reuso de um emissor com o tempo

Permite o reuso de um assunto com o tempo

Campos complementares com informações adicionais personalizadas




Chave Privada da
Autoridade Certificadora


Geração de Assinatura Digital

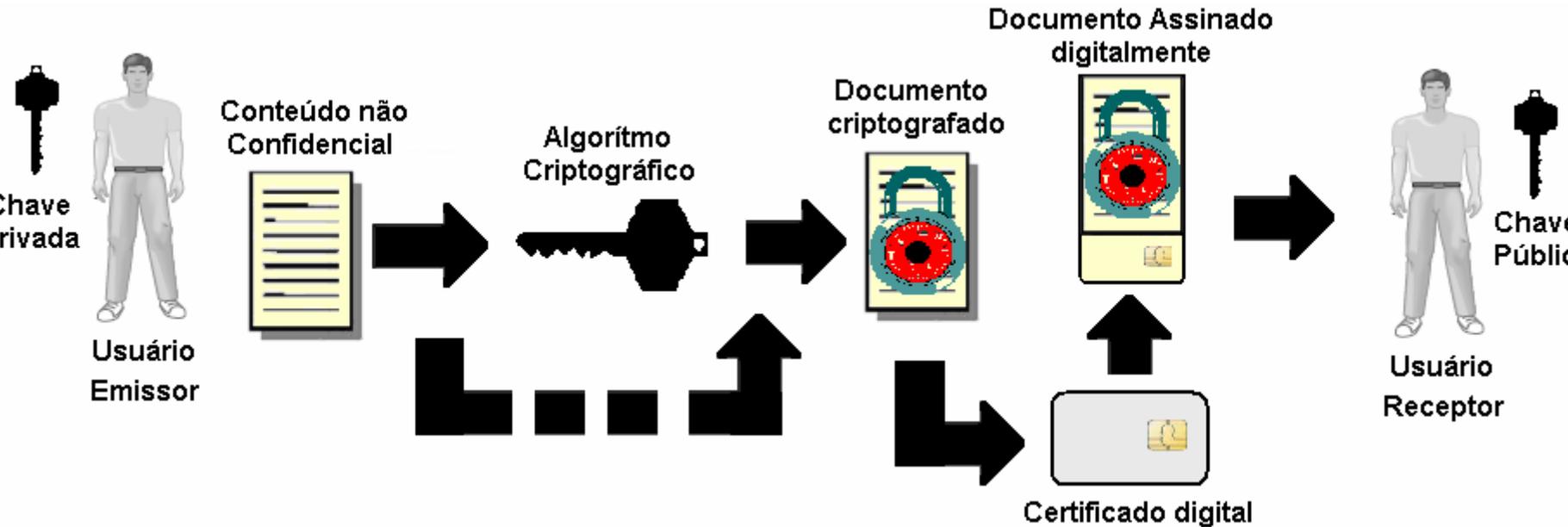
Formato criado pelo ITU-T e ISO/IEC, que proporciona as informações necessárias para identificar o certificado digital.

Assinatura Digital

- Conjunto de procedimentos matemáticos realizados com a utilização de técnicas de criptografia que permite, de forma única e exclusiva, a comprovação da autoria de um determinado conjunto de dados.
- Não é reutilizável, ou seja, a assinatura é uma função do documento e não pode ser transferida para outro documento. Da mesma forma a assinatura não pode ser repudiada.

Assinatura Digital

Processo de Assinatura do Documento



Assinatura Digital

- Versão digital da assinatura de punho em documentos físicos.
- O destinatário pode verificar se a mensagem foi realmente emitida pela pessoa cuja assinatura nela consta, ou se a mensagem foi adulterada intencional ou acidentalmente depois de assinada.

Assinatura Digital

Processo de Verificação da Assinatura

