Certificado Digital

Prof. Dr. Adilson Eduardo Guelfi
guelfi@unoeste.br

Faculdade de Informática de PP
UNOESTE

Agenda

- **Certificado Digital**
- **Transações Seguras Utilizando Certificados Digitais**

Certificado Digital

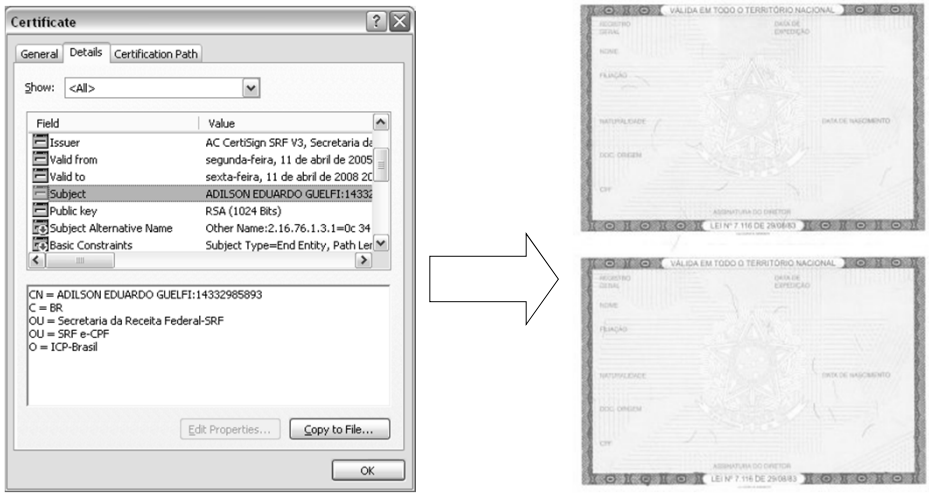
Certificado Digital

- **Documento usado pelos participantes de uma comunicação <u>para a troca confiável de chaves públicas</u>**
- **O certificado digital é assinado digitalmente por uma <u>autoridade certificadora (AC)</u>**
- **Exemplos de Autoridades Certificadoras (ACs)**
  - Internacional
    - Verisign
    - Thawte
  - Brasileira
    - Certisign, SERASA, SERPRO, Boa Vista, VALID etc

Certificado Digital

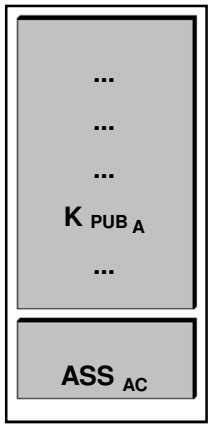
- **Certificado Digital**
  - Documento eletrônico ou objeto de dados que foi criado para prover a autenticidade (confiança) e também vincular o par de chaves (chave pública e chave privada) a uma identidade (pessoa física ou jurídica)
    - Comumente chamado de “Identidade Digital”
  - O certificado digital é assinado digitalmente por uma autoridade certificadora (AC)
    - AC – “Cartório Digital”
  - Passível de verificação eletrônica segura via software
  - Provê segurança às aplicações de assinatura digital

Certificado Digital



Certificado Digital

- **Certificado digital contém campos de Informações:**
  - Identificação do dono do certificado
  - Chave pública do dono do certificado
  - Prazo de validade do certificado;
  - Identificação da AC
  - Número de série
  - Outros
  - Assinatura do certificado pela AC
  - etc

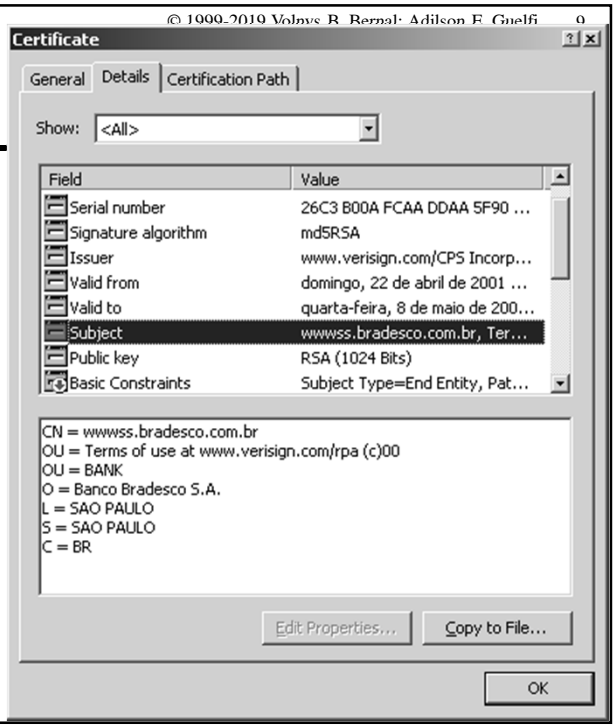


Certificado Digital

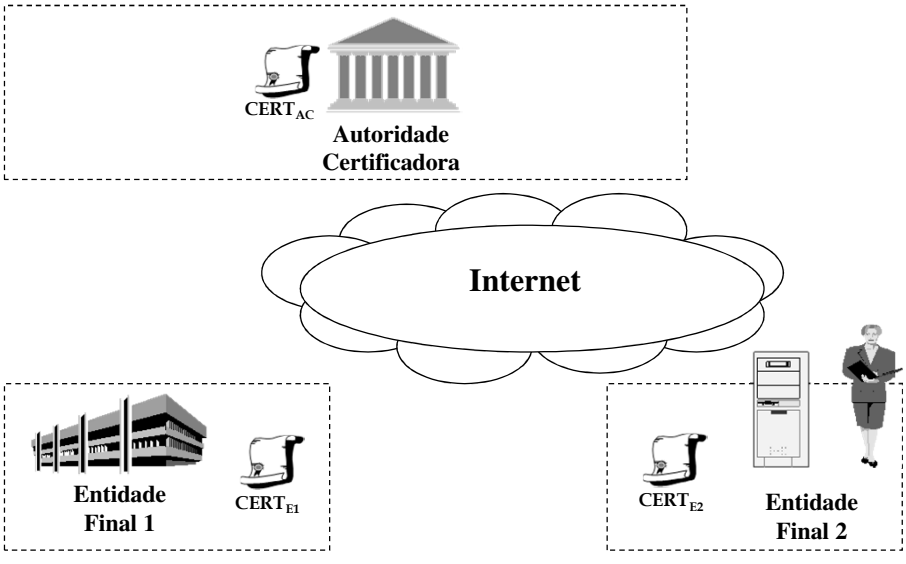
- **Requisitos de um certificado:**
  - Qualquer usuário pode consultar as informações de um certificado digital para determinar o nome e a chave pública do proprietário do certificado
    - Certificado digital é público
  - Qualquer usuário pode verificar a autenticidade de um certificado digital
  - Somente uma AC pode gerar e emitir certificados

Certificado Digital

- Exemplo de certificado digital para servidor



Certificado Digital



Transações Seguras
Utilizando Certificados Digitais

Transações Seguras

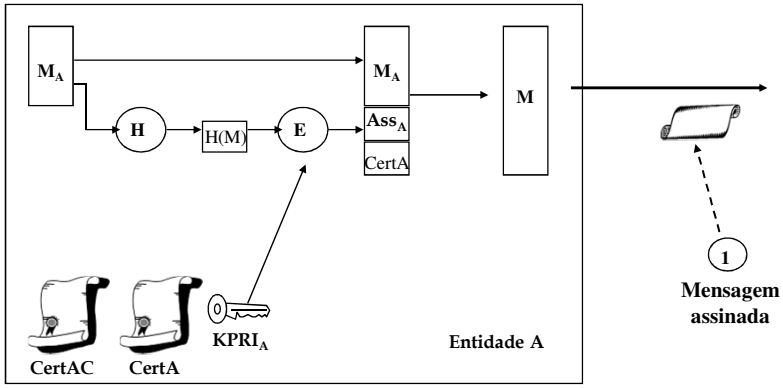
- **O esquema de certificação digital permite a realização de transações seguras pois:**

  (a) Resolve o problema da autenticidade de chaves públicas

  (b) Possibilita acrescentar o serviço de autenticação do parceiro

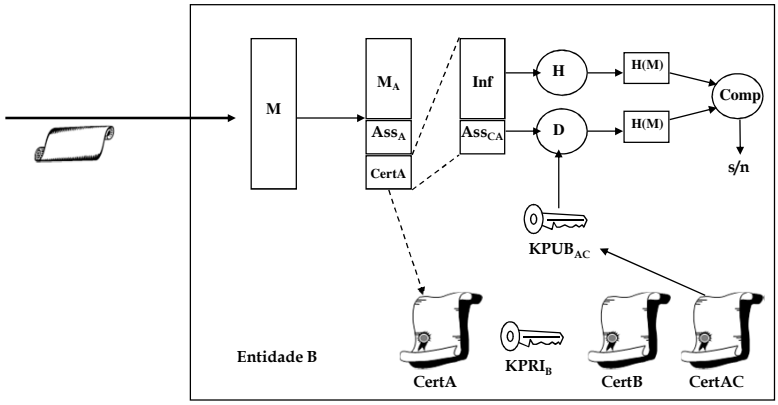
Exemplo de transação

- **Envio de uma mensagem assinada**



Exemplo de transação

- **Recebimento de uma mensagem**
  (a) Verifica o certificado recebido



Exemplo de transação

- **Recebimento de uma mensagem**

  (b) Verifica a assinatura da mensagem