

Assinatura Digital

Prof. Dr. Adilson Eduardo Guelfi[1]
Prof. Dr. Volnys Borges Bernal[2]

(1) Faculdade de Informática de PP
UNOESTE

(2) Laboratório de Sistemas Integráveis
Escola Politécnica da USP

Agenda

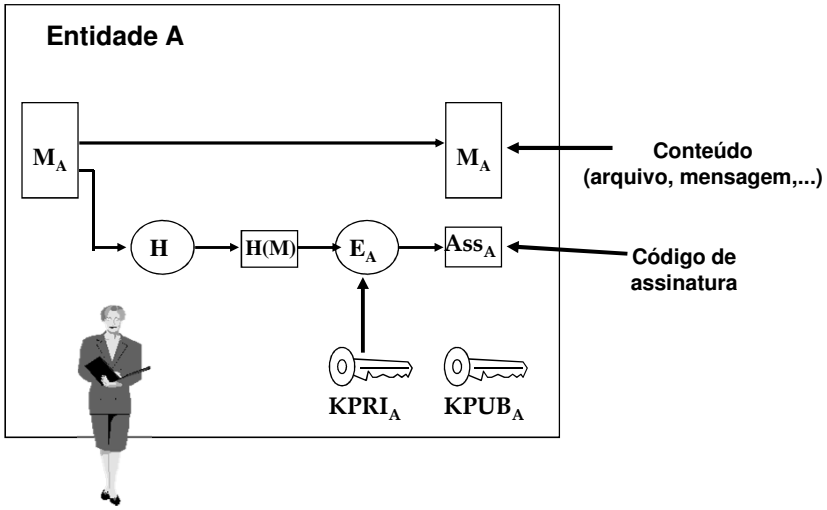
- Esquema de Assinatura Digital
- Assinatura Digital - Propriedades
- Referências Bibliográficas

Esquema de Assinatura Digital

Esquema de Assinatura Digital

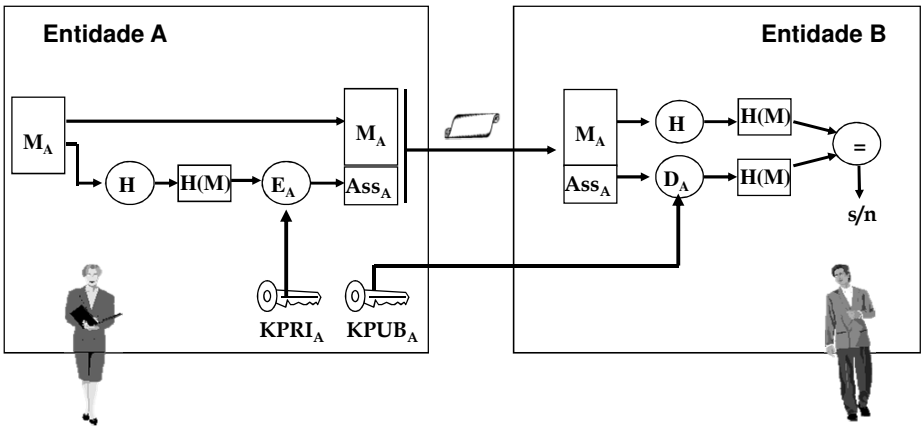
- **Pré-requisitos para uso**
  - Entidade assinante deve possuir um par de chaves assimétricas
    - KPRI - Chave privada
    - KPUB - Chave pública

Esquema de Assinatura Digital



Esquema de Assinatura Digital

- Esquema



Esquema de Assinatura Digital

- **Esquema:**
  - Emissor
    - Emissor criptografa com sua chave privada o código *hash* da mensagem (assinatura).
    - Mensagem assinada é composta pela mensagem e pelo bloco de assinatura
  - Receptor
    - O receptor produz o código *hash* da mensagem recebida e compara com o obtido pela decodificação da assinatura recebida
    - Se forem iguais, a assinatura é aceita como válida.

Assinatura Digital - Propriedades

Assinatura Digital - Propriedades

- **Serviços de segurança oferecidos**
  - Integridade
  - Autenticação de mensagem (autoria)
  - Irretratabilidade de geração
    - Assinante precisa ter seu certificado digital
    - Deve-se pensar em termos de ato que pode ser matematicamente verificado

Assinatura Digital – Propriedades

- **Propriedades**
  - Integridade:
    - A assinatura depende da mensagem assinada
    - Qualquer alteração da mensagem é acusada na verificação da assinatura
  - Autoria e irretratabilidade de geração
    - A assinatura usa uma informação exclusiva, secreta e única que está associada à entidade assinante (chave privada)
      - Possibilita verificar a entidade assinante
      - Evita irretratabilidade de geração

Assinatura Digital – Propriedades

- **Propridades (cont.)**
  - Deve verificar autor, data e hora da assinatura
  - Deve autenticar o conteúdo no momento da assinatura
  - Deve ser relativamente fácil produzir a assinatura digital
  - Deve ser relativamente fácil verificar a assinatura digital, inclusive por terceiros
  - Deve ser computacionalmente inviável falsificar uma mensagem assinada digitalmente
    - Gerando uma nova mensagem para uma assinatura eletrônica existente
  - O armazenamento da mensagem assinada e da própria assinatura (ou cópias delas) deve ser possível e prático

Assinatura Digital - Propriedades

- **Desvantagens**

  (1) Toda a segurança do processo depende do segredo da chave privada do transmissor
    - Se a chave privada for perdida ou roubada, o transmissor poderia repudiar a transmissão / geração de uma mensagem particular

  (2) NÃO GARANTE O INSTANTE DA ASSINATURA!
    - Afeta documentos eletrônicos assinados digitalmente
    - Problema temporal da revogação da chave

  (3) Vulnerável a ataques de “replay”

  (4) **Depende de uma função hash considerada segura, ou seja, resistente a colisões**

Referências Bibliográficas

Referências Bibliográficas

- **Criptografia e Segurança de Redes - Princípios e Práticas (4a. Edição)**
  - Willian Stallings, Pearson. 2008
- **APPLIED CRYPTOGRAPHY - PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C**
  - SCHNEIER, BRUCE, Editora: JOHN WILEY CONSUMER, Edição: 2ª, 1996