UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Segurança da Informação
Aula 8 – Certificação Digital

Prof. Dr. Eng. Fred Sauer

http://www.fredsauer.com.br

fsauer@gmail.com

Certificação Digital
Introdução

- **Uma vulnerabilidade não resolvida até aqui:**
  - **Suponha que Bob e Alice vão se falar pela primeira vez.**
  - **Ambos devem obter a chave pública do outro.**
  - **Se um terceiro (Trudy) consegue distribuir chaves falsas para ambos:**
    - **Trudy poderia intermediar (e interceptar) toda a comunicação entre Bob e Alice.**
    - **Bob e Alice pensariam estar se comunicando diretamente e com segurança, mas não seria a realidade.**

Certificação Digital
Introdução

- Justificativa
- Usuário de chaves públicas
  - Originador de uma mensagem criptografada
    - Precisa conhecer a chave pública do destinatário
  - Destinatário de uma mensagem autenticada
    - Precisa conhecer a chave pública do originador
  - É necessário que o usuário tenha certeza de que a chave pública que está utilizando é autêntica.
    - Pequeno grupo – poderia trocar as chaves públicas e guardá-las de forma segura.
    - Grande grupo – troca manual de chave é impraticável.

Certificação Digital

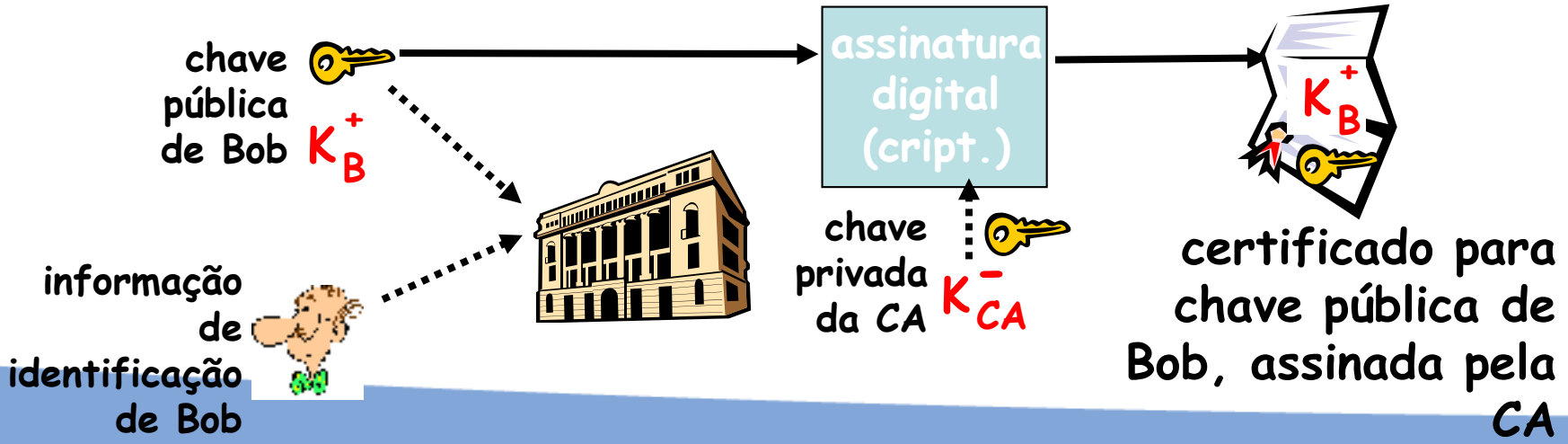
- **Certificado Digital** - arquivo digital que contém as informações necessárias à identificação de um indivíduo ou programa, equipamento, componente, produto, etc, incluindo sua chave pública;

- **Principal função de um certificado** – vincular uma chave pública ao nome de um protagonista (indivíduo, empresa, etc.).

- Os certificados em si não são secretos ou protegidos. Usualmente estão disponíveis em uma base de acesso livre na Internet (diretório X.500).

Autoridades de Certificação

- **Autoridade Certificadora (AC):** vincula chave pública à entidade particular, “E”.
- “E” (pessoa, roteador) registra sua chave pública com CA.
  - “E” fornece “prova de identidade” à CA.
  - CA cria certificado vinculando “E” à sua chave pública.
  - certificado contendo chave pública de “E” assinada digitalmente pela CA – CA diz: ***esta é a chave pública de “E”***



Certificação Digital

- **Autoridade Certificadora (AC)**
  - CA (**Certification Authority**) - cartório eletrônico.
  - Entidade que emite certificados para possuidores de chaves públicas e privadas (pessoa, dispositivo, servidor).

- Atribuições de uma CA:
  - Gerar, entregar e armazenar a chave privada de forma segura;
  - Distribuir a chave pública;
  - Atualizar o par de chaves;
  - Assinar a chave pública para gerar o certificado. Assinar certificados digitais garantindo sua validade
  - Manter e divulgar uma lista com os certificados revogados (Certificate Revocation List - CRL);
  - CAs podem estar encadeadas em hierarquias de certificação, em que a CA de um nível inferior valida sua assinatura com a assinatura de uma CA mais alta na hierarquia.

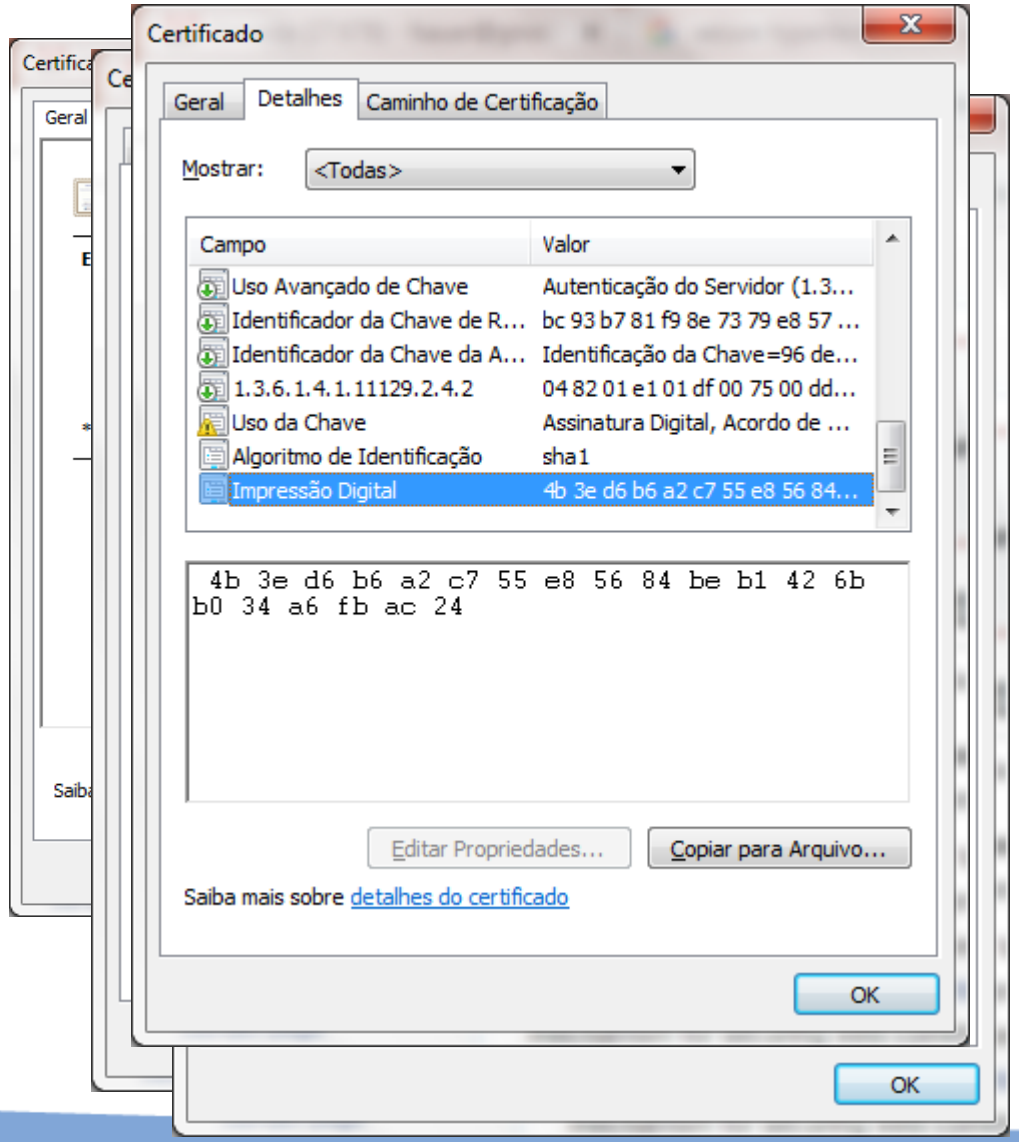
- **Exemplos de CAs**: VeriSign e Cybertrust.

Certificação Digital

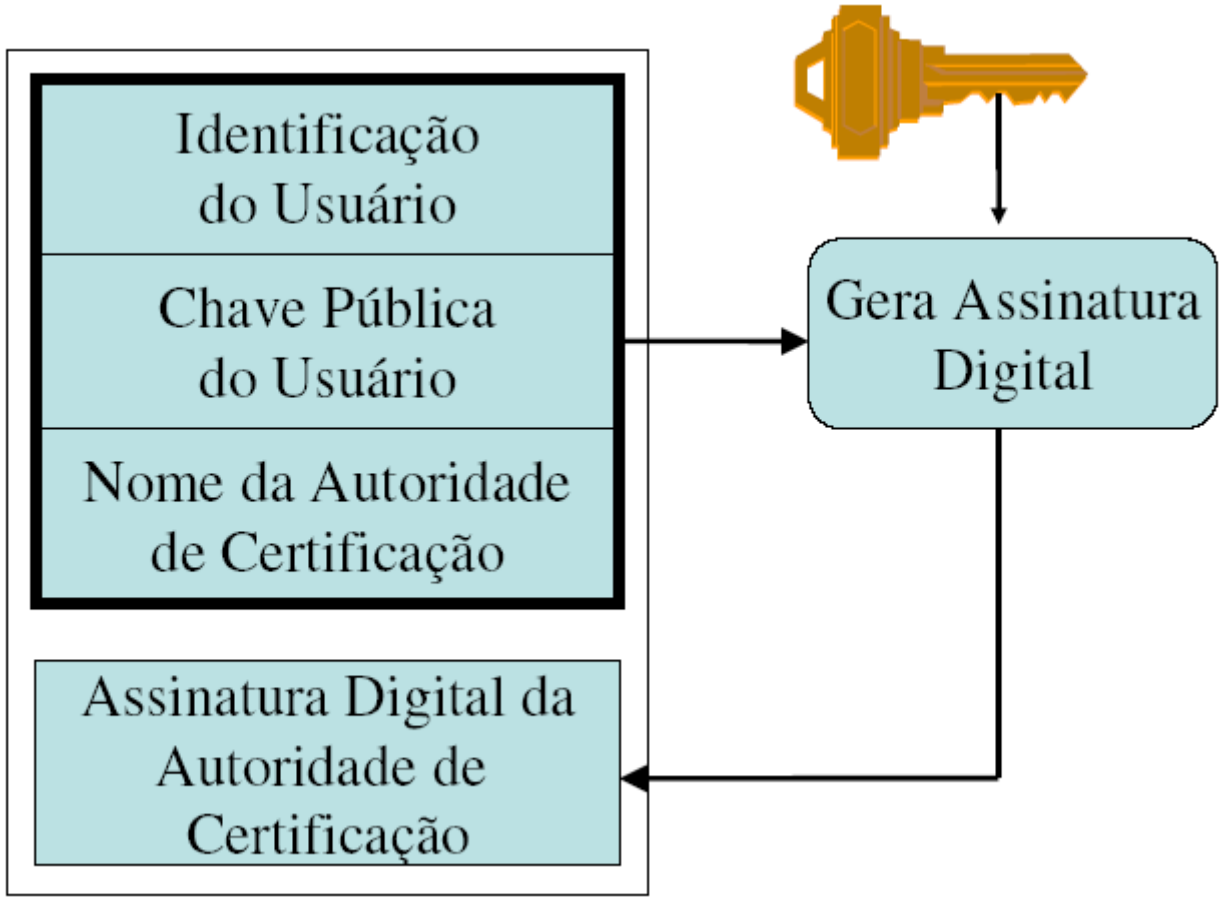
- **Período de validade e revogação**
- Os certificados definem períodos de validade para as chaves públicas.
- Certificados podem ser revogados antes de sua expiração:
  - **Suspeita de comprometimento da chave privada**
  - **Término de contrato**
  - **Mudança de nome**

Certificação Digital

- Componentes básicos de um certificado digital:
  - A chave pública;
  - Nome e endereço de e-mail;
  - Data da validade da chave pública;
  - Nome da autoridade certificadora (CA);
  - Número de série do Certificado Digital;
  - Assinatura Digital da Autoridade Certificadora.



Certificação Digital



Certificação Digital

- Para que serve um Certificado Digital?
  - Correio Eletrônico seguro
  - Transações Bancárias sem repúdio
  - Compras pela Internet sem repúdio
  - Consultas confidenciais a cadastros
  - Arquivo de documentos legais digitalizados
  - Transmissão de documentos
  - Contratos digitais
  - Certificação de Equipamentos
  - Certificação de Programas de Computador
  - Certificação de vídeo, som e comandos digitais

Certificação Digital

- **Obtenção de um Certificado**
  - Cliente gera um par de chaves pública e privada (por exemplo, usando RSA);
  - Envia-se um pedido de certificado para a Autoridade de Registro;
  - AR (Autoridade Regional de Registro) faz a prova de existência do requisitante e retransmite o pedido para a AC;
  - AC assina e envia o certificado;
  - Usuário instala seu certificado;
  - Usuário divulga o certificado.

Certificação Digital

- **Política de Certificação**

- A Autoridade de registro (AR), tendo a delegação de uma AC para tal, faz uma investigação no solicitante e determina:
  - Se o pedido deve ser atendido;
  - Quais as características que deve ter.

Certificação Digital

- **Tipos de certificados**
  - **Certificados de CA**: utilizados para validar outros certificados; auto-assinados ou assinados por outra CA.
  - **Certificados de servidor**: utilizados para identificar um servidor seguro; contém o nome da organização e o nome DNS do servidor.
  - **Certificados pessoais**: contém nome do portador e, eventualmente, informações como endereço eletrônico, endereço postal, etc.
  - **Certificados de desenvolvedores de software**: utilizados para validar assinaturas associadas a programas.

Certificação Digital

- Distribuição dos Certificados
  - **Assinatura digital**
    - O certificado pode acompanhar o dado assinado.
  - **Criptografia**
    - Remetente precisa obter a chave pública certificada do destinatário
    - Serviço de diretório
      - X.500, NDS, Lotus Notes, Microsoft
    - WEB
    - S/MIME

Certificação Digital

- **Requisitos para uma Infraestrutura de Chave Pública**

- Requisitos Básicos
  - Escalabilidade
  - Suporte a várias aplicações
  - Interoperabilidade
  - Suporte a múltiplas políticas
  - Limitação de responsabilidade
  - Padronização

Certificação Digital

- Infraestrutura para o gerenciamento de chaves públicas - padrão **Public Key Infrastructure** (PKI), determina:
  - Onde os certificados digitais serão armazenados e recuperados, de que forma estão armazenados, como um certificado é revogado, etc.
  - No Brasil, é regulada via decreto pelo ITI - http://www.iti.gov.br

Certificação Digital

- **Função da PKI**
  - Fornecer um modo para estruturar os componentes (usuários, CAs, certificados, etc.).
  - Definir padrões para os vários documentos e protocolos.
  - Garantir a autenticação, confidencialidade, integridade e a não recusa das informações.
    - **Exemplo**: uma empresa pode usar a PKI para controlar o acesso a rede de computadores. No futuro, as empresas poderiam usar a PKI para controlar o acesso, desde a entrada nos prédios até a obtenção de mercadorias.

Fixação

- A grande vantagem do uso de uma PKI é que o servidor de chaves não precisa ter acesso à chave **Privada** dos usuários.
- Apesar da emissão do certificado ser uma responsabilidade de uma **AC**, a prova de identidade do usuário é feita junto à uma **AR**.
- Uma importante informação no certificado digital é a sua prova de integridade e autenticidade, obtida através de sua **Impressão Digital**. Essa informação é produzida através da criptografia assimétrica do **Hash do Certificado** através da **Chave Privada** da AC.
- O órgão brasileiro responsável pela regulação da PKI é o **ITI**.