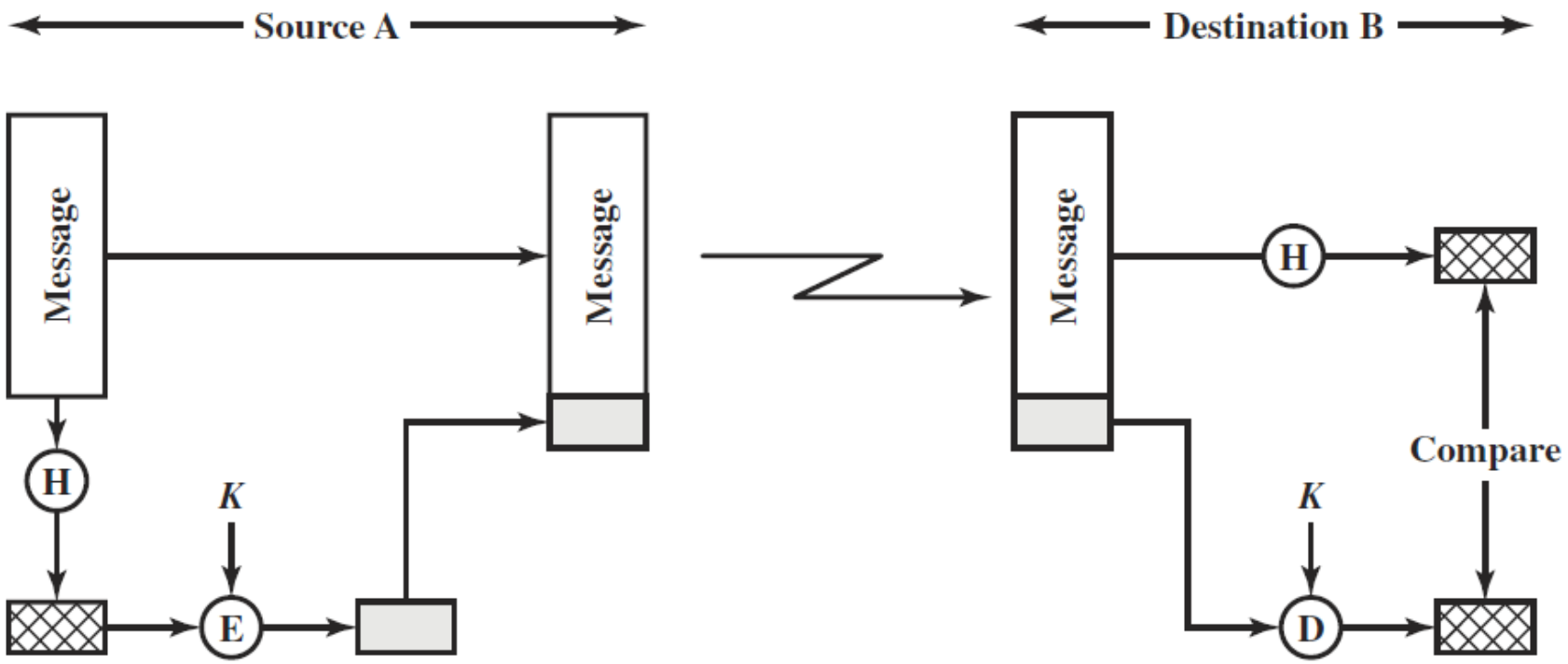
Segurança da Informação– GBC083

Prof. Rodrigo Sanches Miani – FACOM/UFU

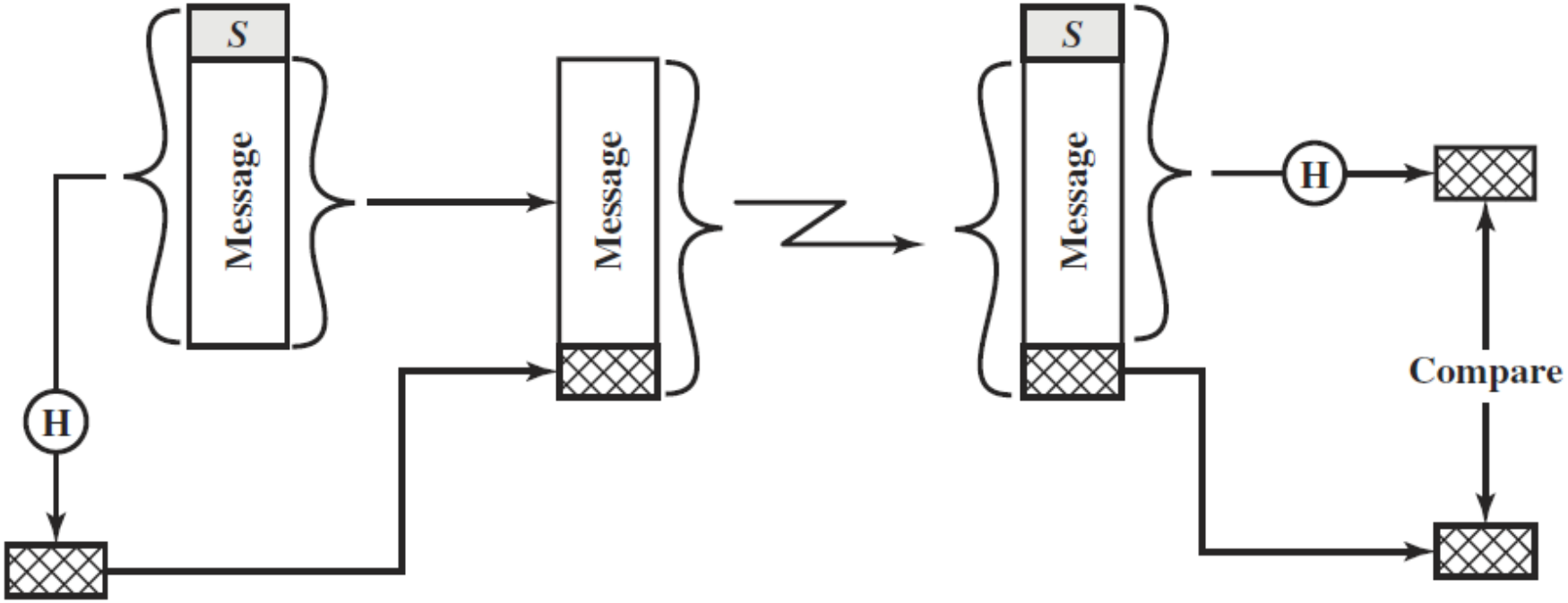
Aulas passadas

Segurança da Informação– GBC083

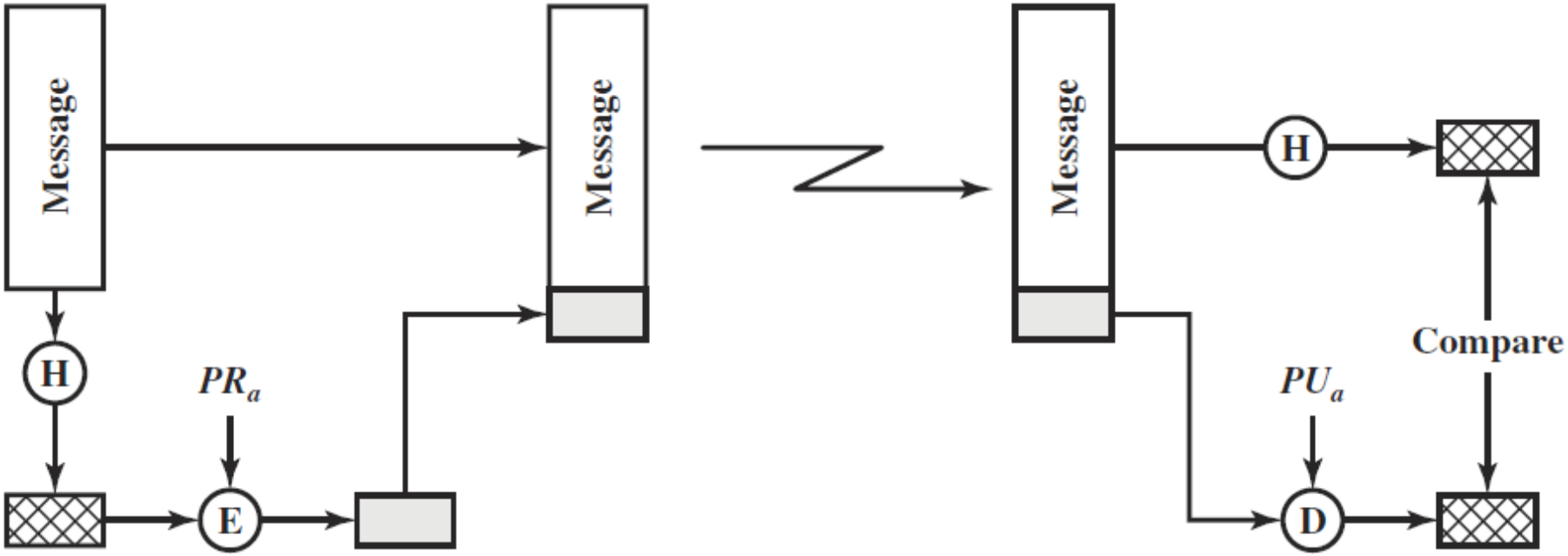
Autenticação usando função hash - 1



Autenticação usando a função hash - 2



Assinatura digital – Funcionamento básico



Tópicos da aula

Segurança da Informação– GBC083

Tópicos da aula – Integridade e autenticação

1. Assinatura digital
2. Certificados digitais
3. Gerenciamento de certificados (PKI/AC)
4. Conferência de certificados
5. X509

Assinatura digital

Segurança da Informação– GBC083

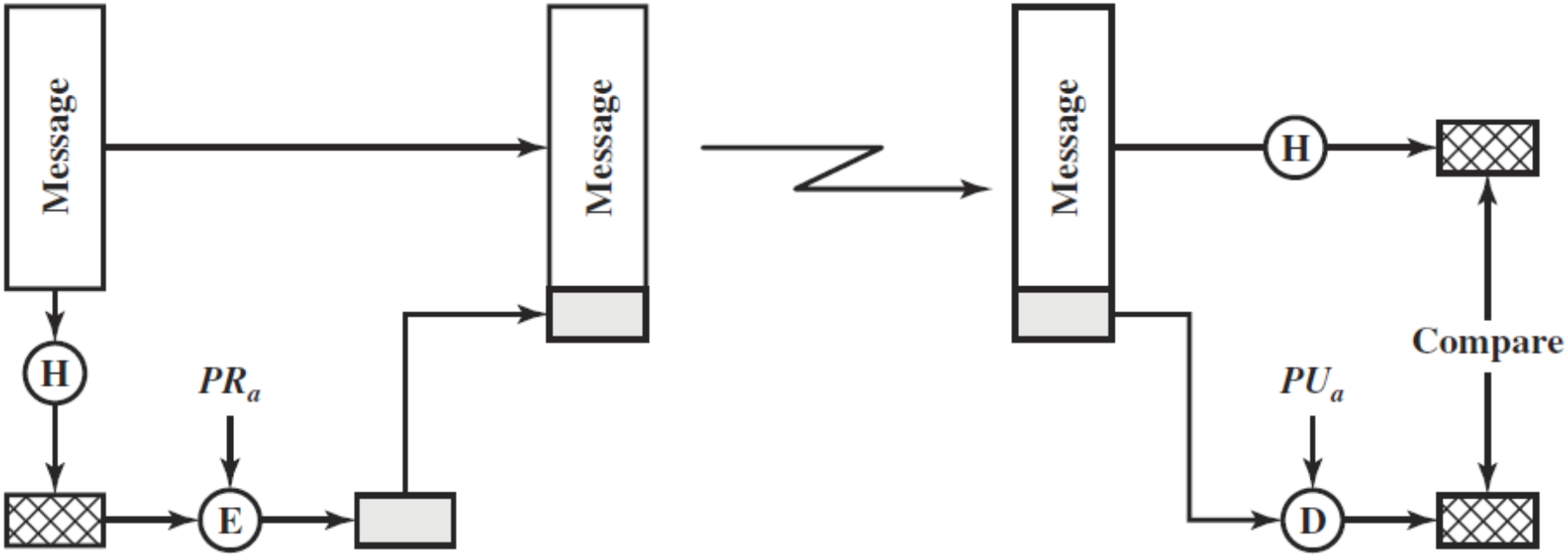
Características

- Assinatura digital procurar resolver o problema em situações onde somente a autenticação não é suficiente;
  - Não existe confiança mútua entre emissor e receptor.

- As seguintes características são desejáveis:
  1. Verificar o **autor** da assinatura;
  2. **Autenticar** o conteúdo no momento da assinatura;
  3. Ser verificável por **terceiros**, para resolver disputas.

- Vamos relembrar o que sabemos sobre assinatura digital...

Assinatura digital – Funcionamento básico



Características

Algumas perguntas interessantes...

1. É possível verificar o autor?
2. O conteúdo está autenticado?
3. Um terceiro poderia verificar o procedimento?

Características

Algumas perguntas interessantes...

1. É possível verificar o autor? *Sim! Chave privada/chave pública...*
2. O conteúdo está autenticado? *Sim! Hash da mensagem + cifra com a chave privada.*
3. Um terceiro poderia verificar o procedimento? *Se o terceiro souber que a chave pública do emissor realmente é dele, seria possível verificar o procedimento.*

Divulgação de chaves públicas

- A natureza das chave públicas faz com que seja importante divulgá-las amplamente.

- Indivíduos podem anunciar suas chaves livremente:
  - **Problema**: como garantir que aquela chave pública realmente pertence a uma determinada entidade?

Divulgação de chaves públicas – Possível solução

Entidades confiáveis podem se encarregar de administrar um **diretório** de chaves públicas, garantindo a procedência da chave pública...

Divulgação de chaves públicas - Divulgação de chaves públicas – Possível solução

- Entidades confiáveis podem se encarregar de administrar um diretório de chaves públicas, garantindo a procedência da chave pública:
  - Problemas:
    - consultar o diretório toda vez que precisa utilizar a chave pública pode ser um gargalo.
    - Se o diretório for comprometido, todos os envolvidos estarão em risco.
- Solução adotada na prática: certificados digitais.

Certificado digital

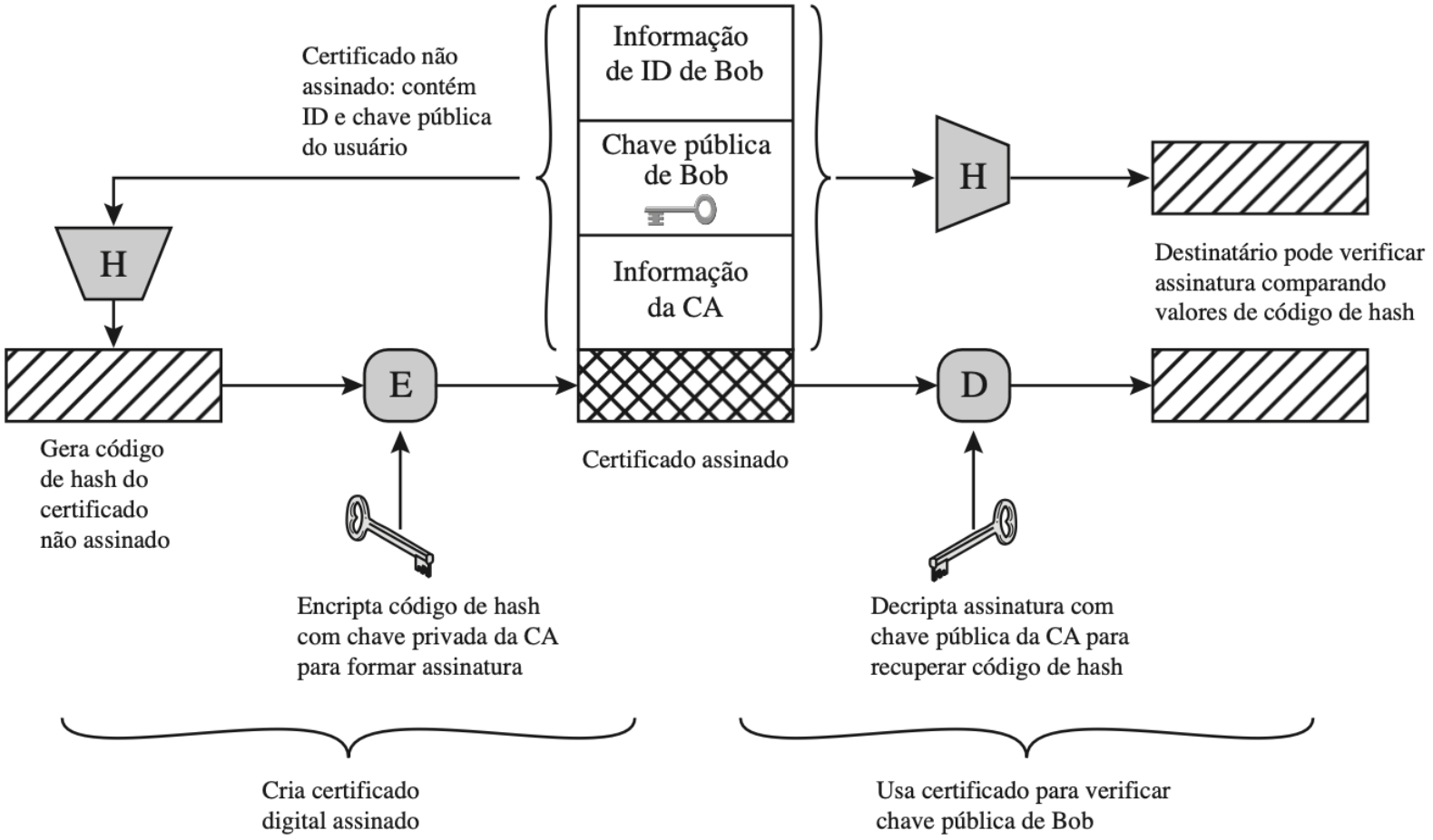
Segurança da Informação– GBC083

Certificados digitais

- Certificados digitais utilizam a criptografia de chave pública (criptografia assimétrica).

- Definição rápida de certificado digital:
  - Chave pública de um usuário ou sistema que é assinada digitalmente por uma autoridade certificadora (AC) usando a chave privada dela.

Certificado Digital



Certificado digital

- Um certificado digital pode conter diversas informações:
  - Nome, endereço e empresa do solicitante.
  - Chave pública do solicitante.
  - Validade do certificado (muito importante).
  - Nome e endereço da autoridade certificadora.
  - Políticas de utilização.

Certificado digital

Existe um terceiro (AC) que irá assinar as chaves públicas, gerando um certificado para elas...

- Como esse processo de assinatura é feito?
- Quem é essa AC?
- Como os certificados são gerenciados?

Gerenciamento de certificados

Segurança da Informação– GBC083

Autoridades Certificadoras

- As Autoridades Certificadoras (AC) têm a função de criar, manter e controlar todos os certificados que elas emitem;

- Elas devem, inclusive, invalidar certificados expirados ou comprometidos;

- O gerenciamento de certificados digitais e o papel de uma AC são assuntos complexos e delicados.
  - Ambos são analisados dentro do assunto conhecido como Infraestrutura de chaves pública – PKI.

Infra-estrutura de chave pública

- PKI: Public Key Infrastructure;

- É uma união de pessoas, organizações, hardware, software, políticas e procedimentos para prover a infraestrutura necessária ao uso adequado de certificados digitais baseados em chaves públicas;
  - Exemplo: ICP-Brasil - https://www.iti.gov.br/icp-brasil

- Uma PKI oferece confiabilidade nas transações que utilizam certificado digital.

Infra-estrutura de chave pública – ICP-Brasil

- ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão;

- O modelo adotado pelo Brasil foi o de certificação com raiz única;
  - Desempenha o papel de Autoridade Certificadora Raiz – AC-Raiz;
  - Também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

Infra-estrutura de chave pública – ICP-Brasil

- É gerida pelo Instituto Nacional de TI, que é uma autarquia federal ligada à Casa Civil da presidência da República;

- A ICP-Brasil é dirigida por um comitê gestor formado por representantes de diferentes setores da sociedade nomeados pela presidência da república.

Infra-estrutura de chave pública – ICP-Brasil

- A ICP-Brasil está dividida em três níveis: raiz, nível 1 e nível 2;
- Hierarquia: os maiores reconhecem os menores e a AC raiz é **auto assinada**, ninguém certifica ela;
- A figura a seguir ilustra a estrutura da ICP-Brasil atual;
  - https://estrutura.iti.gov.br
  - Existem ACs e ARs (responsável pela interface entre o usuário e a Autoridade Certificadora).

ICP-Brasil - Exemplo

Funções da AC

1. Registro: uma entidade se registra em uma AC por meio de uma Autoridade de Registro (AR – Registration Authority).

2. Certificação: a AC envia o certificado digital para a entidade que requereu e o coloca em um repositório (diretório).

3. Recuperação do par de chaves: a AC pode guardar uma cópia de segurança da chave privada da entidade e fornecê-la em caso de necessidade.

Funções da AC

4. Geração de chaves: pode ser feita pelo próprio usuário ou pela AC;

5. Atualização das chaves: quando a chave é comprometida ou expira;

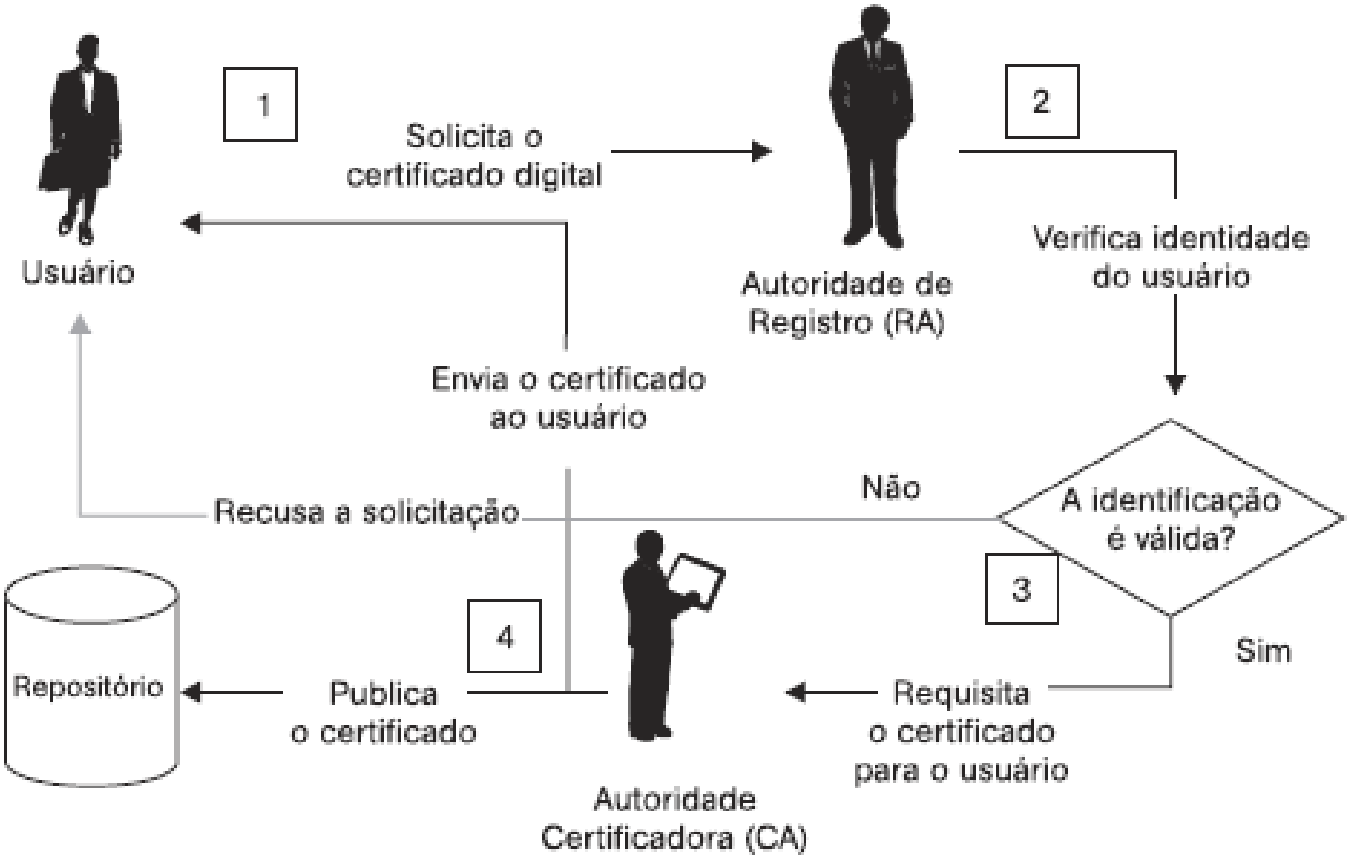
6. Revogação: o certificado pode ser revogado em caso de comprometimento do certificado, mudanças no nome da entidade, etc. Certificados revogados devem ser incluídos em uma lista pública;

7. Distribuição e publicação de certificados e de notificações de revogação.

Infra-estrutura de chave pública – Perguntas

Suponha que vocês abriram um e-commerce e precisam se adequar a ICP-Brasil. O que fazer?

Solicitação de certificado digital



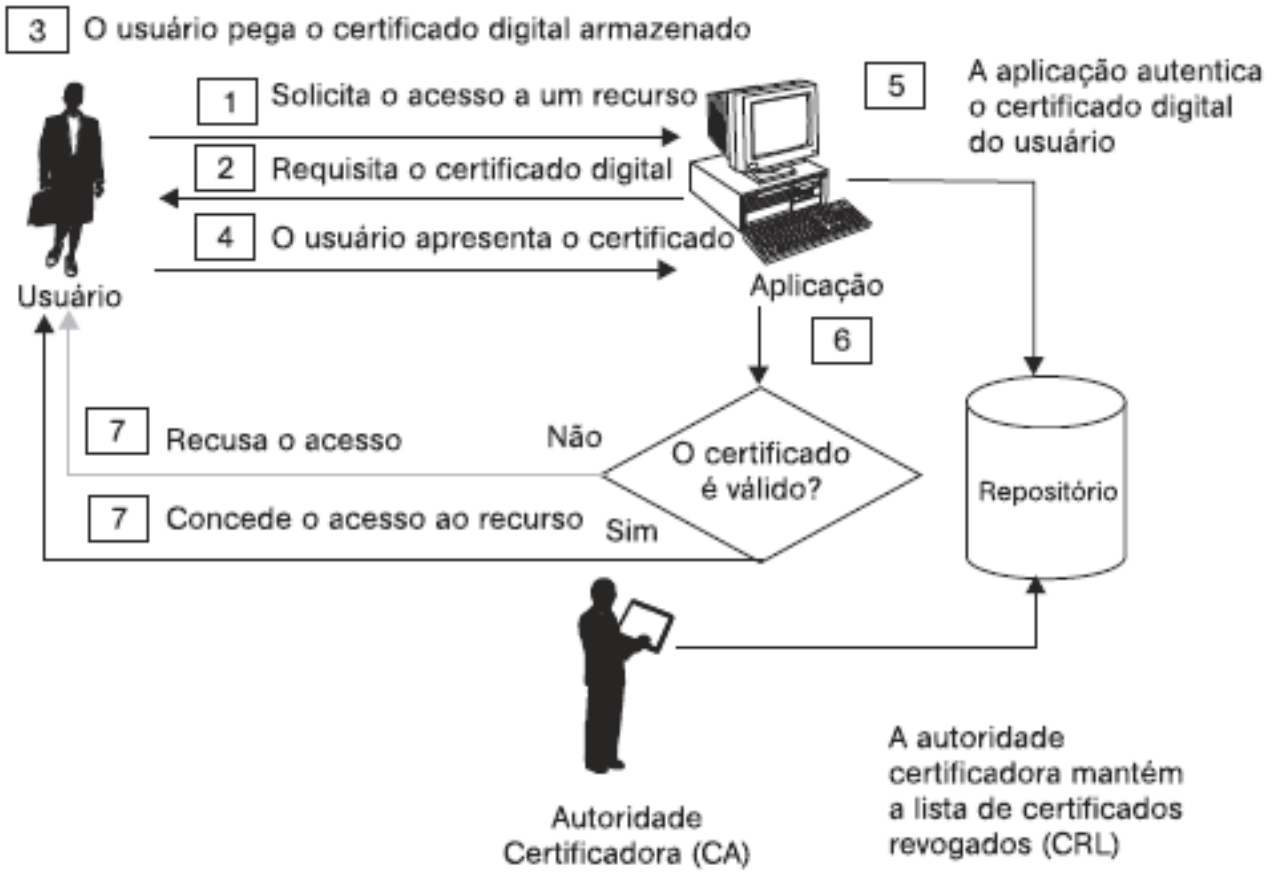
Infra-estrutura de chave pública – Perguntas

Suponha que vocês abriram um e-commerce e precisam se adequar a ICP-Brasil. O que fazer?

Solicitar em certificado! Quanto será que vai custar a "brincadeira"?

https://loja.certisign.com.br

Acesso a recurso utilizando a PKI



PKI – Perguntas

1. Qual o problema dos certificados grátis? *Let's Encrypt* é um exemplo.
2. Qual o problema dos certificados autoassinados?

Infra-estrutura de chave pública – Perguntas

Qual o problema dos certificados grátis? Let's Encrypt é um exemplo.

- Como é o processo de verificação? Quem assina? O que acontece se um agente malicioso gera um certificado desses e disponibiliza um site que não armazena corretamente os seus dados pessoais? Trecho do site: *"Our services are free and easy to use so that* ***every website*** *can deploy HTTPS."*

https://securityboulevard.com/2019/01/lets-encrypt-are-enabling-the-bad-guys-and-why-they-should/

Infra-estrutura de chave pública – Perguntas

Qual o problema dos certificados autoassinados?

- Um atacante pode criar um certificado autoassinado e utilizar, por exemplo, emails contendo *phishing* para induzir os usuários a instalá-lo. A partir do momento em que o certificado for instalado no navegador, passa a ser possível estabelecer conexões cifradas com *sites* fraudulentos, sem que o navegador emita alertas quanto à confiabilidade do certificado.

Conferência de certificados

Segurança da Informação– GBC083

Conferência de certificado (chave pública)

Suponha que Alice e Bob irão se comunicar utilizando a infraestrutura de chaves públicas. Como seria o passo a passo, desde a criação das chaves/certificado até a verificação do mesmo?

Conferência de certificado (chave pública)

1. Bob solicita a criação de um par de chaves para AC;

2. AC verifica a identidade de Bob e, se tudo estiver correto, ela irá gerar um par de chaves (PU_{bob}, PRI_{bob});

3. A AC então irá assinar a chave pública de Bob que ela acabou de gerar fazendo o seguinte: gerar o hash de PU_{bob} - $H(PU_{bob})$ e cifrar esse hash com a sua chave privada (AC) resultando: $Cert_{bob} = E(PRI_{ac}, H(PU_{bob}))$;

4. A AC envia para Bob o seu par de chaves (PU_{bob}, PRI_{bob}) e a assinatura de sua chave pública $Cert_{bob} = E(PRI_{ac}, H(PU_{bob}))$;

Conferência de certificado (chave pública)

5. Em seu navegador, Alice já possui a chave pública da AC - PU_{ac}. Quando Bob tentar conversar com a Alice pela primeira vez, ele irá enviar a sua chave pública PU_{bob} juntamente com o seu certificado $Cert_{bob} = E(PRI_{ac}, H(PU_{bob}))$;

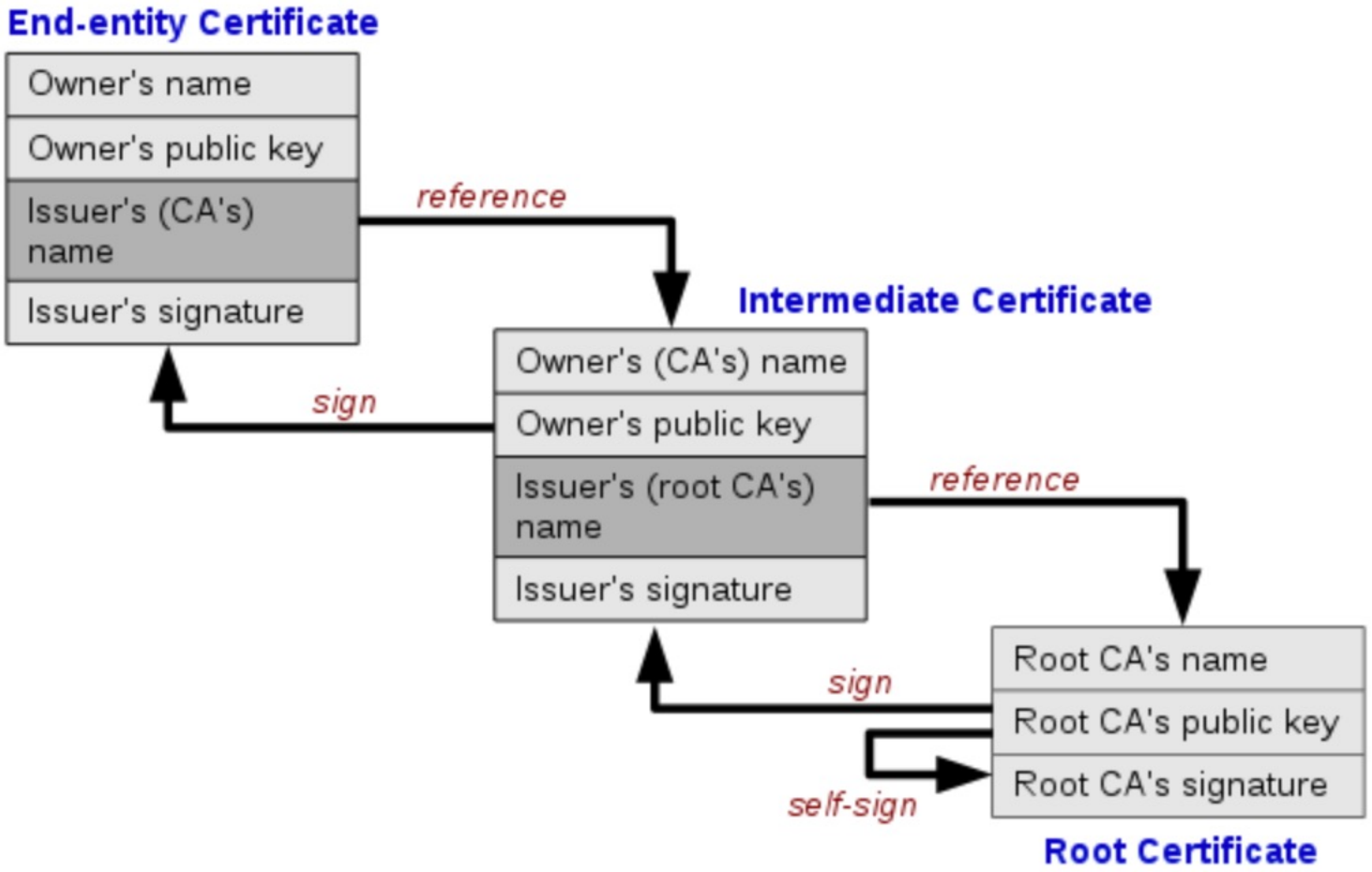
6. Alice recebe PU_{bob} || $Cert_{bob}$. Primeiramente, ela irá calcular o hash de PU_{bob} -> $H(PU_{bob})$* e guardar o resultado. Depois irá usar a chave pública da AC que está instalada no seu navegador para decifrar $Cert_{bob}$ fazendo o seguinte: $D(Cert_{bob}, PU_{ac})$. O resultado dessa operação será $H(PU_{bob})$**. Se $H(PU_{bob})$* = $H(PU_{bob})$**, a chave foi conferida e Alice pode confiar que realmente veio de Bob, pelo intermédio de um terceiro que ambos confiam..

Encadeamento - exercício

Alice irá comprar na loja eletrônica de Bob. Suponha que Alice instalou em seu navegador o certificado da AC raiz. Considere que o certificado de Bob foi obtido com a AC intermediária e que a AC raiz assinou o certificado da AC intermediária.

Nesse cenário, o que deverá ser feito para que Alice verifique o certificado de Bob? Explique e mostre cada um dos passos.

Conferência de certificado – encadeamento



- https://en.wikipedia.org/wiki/Chain_of_trust

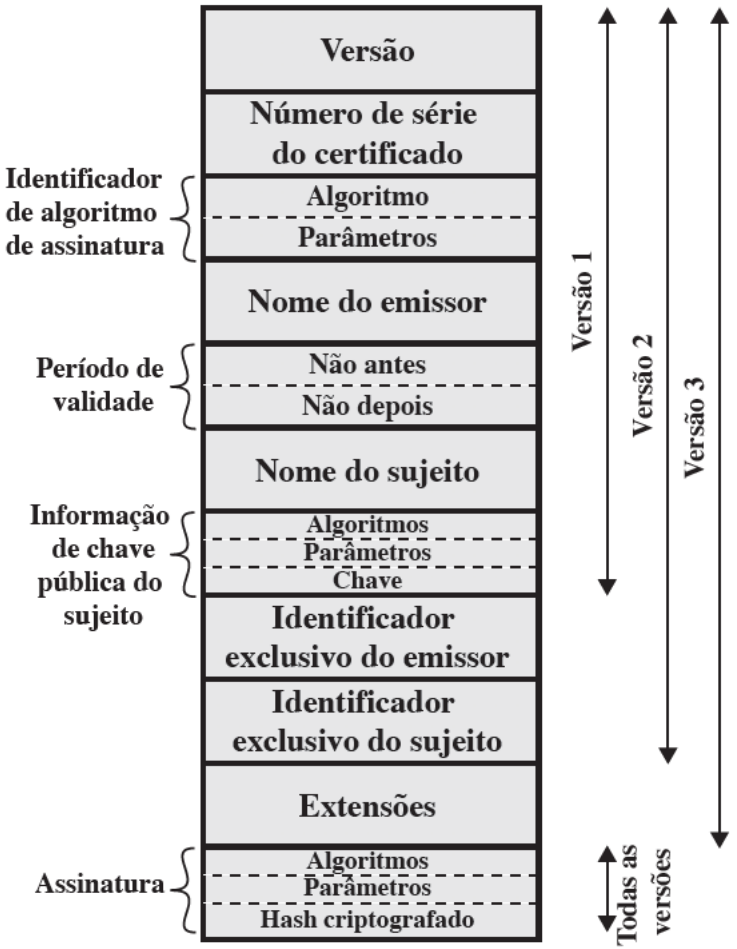
X509

Segurança da Informação– GBC083

X.509

- A recomendação ITU-T X.509 faz parte da série de recomendações X.500, que define serviços baseados em diretórios;
  - O diretório, nesse caso, armazena certificados digitais;
- X.509 v3 é definido na RFC 5280;
  - Essa recomendação padroniza a forma com que os certificados serão armazenados e manipulados em uma infraestrutura de chaves pública.
- Certificados X.509 são usados em protocolos como o TLS.
- https://cryptography.io/en/latest/x509/

X.509



(a) Certificado X.509

X.509

- Versão: versão do formato do certificado (1, 2 ou 3);
- Serial number: número único designado pela autoridade certificadora ao certificado;
- Signature algorithm identifier: apresenta o algoritmo utilizado para assinar o certificado. Tem pouca utilidade pois essa informação é incluída em outro campo.

X.509

- Issuer name: nome da CA que criou o certificado;
- Period of validity: datas de início e fim da validade do certificado;
- Subject name: nome da entidade à qual o certificado se refere.

X.509

- Subject's public key information: chave pública e algoritmo de chave pública utilizados pela entidade à qual o certificado se refere;
- Issuer unique identifier: identificação única da CA;
- Subject unique identifier: identificação única da entidade à qual o certificado se refere.

X.509

- Extensions: campos extras relacionados a dados extras da CA e da entidade, políticas e restrições de uso do certificado, etc.

- Signature: assinatura gerada a partir dos outros campos do certificado. Inclui também o algoritmo utilizado.

Roteiro de estudos

1. Leitura das seções 14.4, 14.5 e 14.6. do livro "Criptografia e segurança de redes. Princípios e práticas". William Stallings;
2. Estudo da vídeo-aula referente ao tópico 13;
3. Abrir diferentes navegadores e procurar pelos certificados instalados neles – qual algoritmo foi usado para assinar? Qual o tamanho da chave? Quem é a AC?
4. Resolução dos TP-5 e TP-6.