UNIVERSIDADE FEDERAL DE ITAJUBÁ

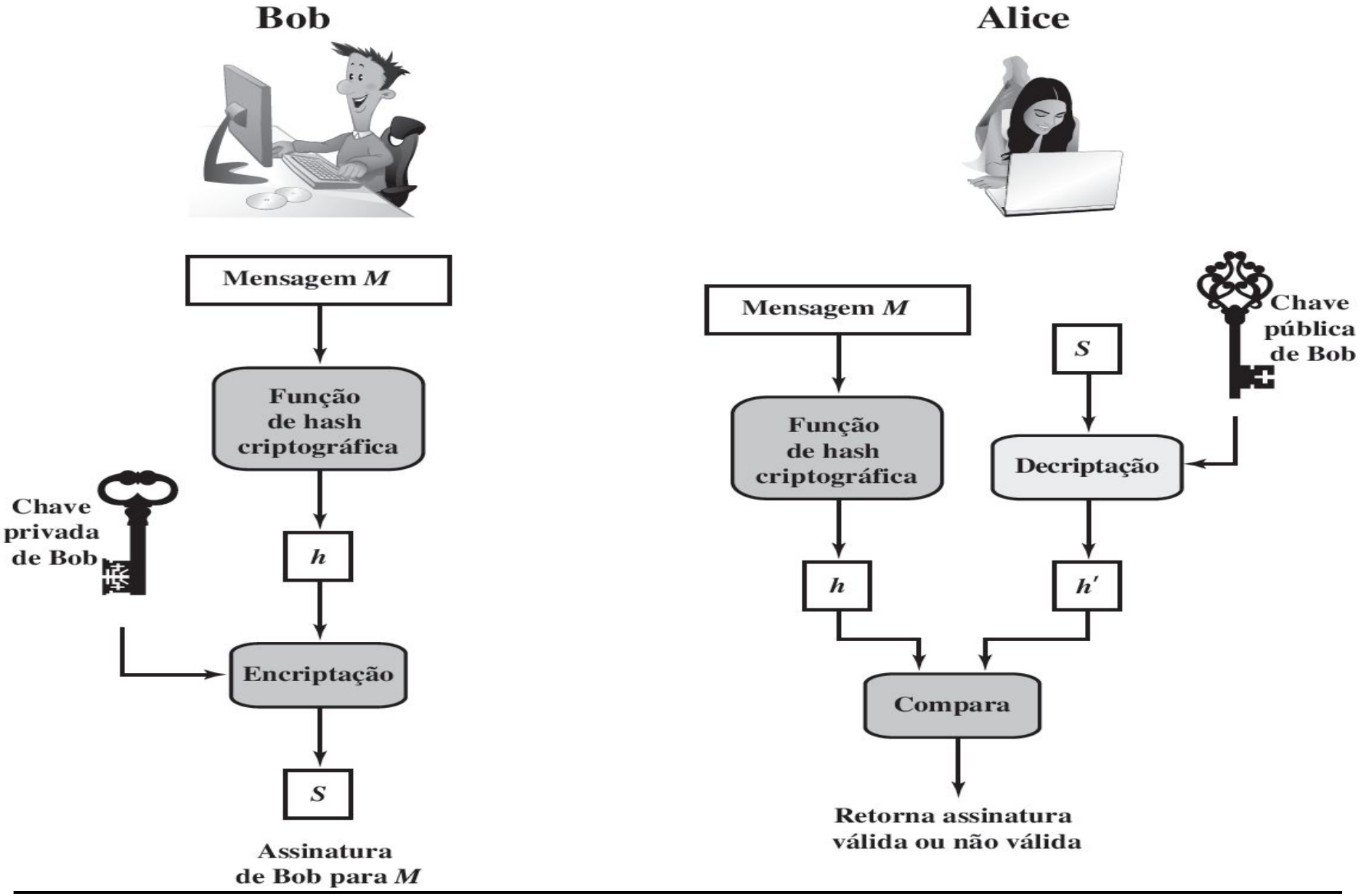
Auditoria e Segurança de Sistemas de Informação

Assinaturas Digitais e Gerenciamento e Distribuição de Chaves

Bruno Guazzelli Batista

brunoguazzelli@unifei.edu.br

Elementos Essenciais



Assinaturas Digitais

Considere as seguintes disputas referentes a figura anterior:

- Mary pode forjar uma mensagem diferente e reivindicar que ela veio de John.
- John pode negar o envio da mensagem.

Em situações nas quais não existe confiança completa entre emissor e receptor, é necessário algo mais do que a autenticação → algoritmo de Assinatura Digital.

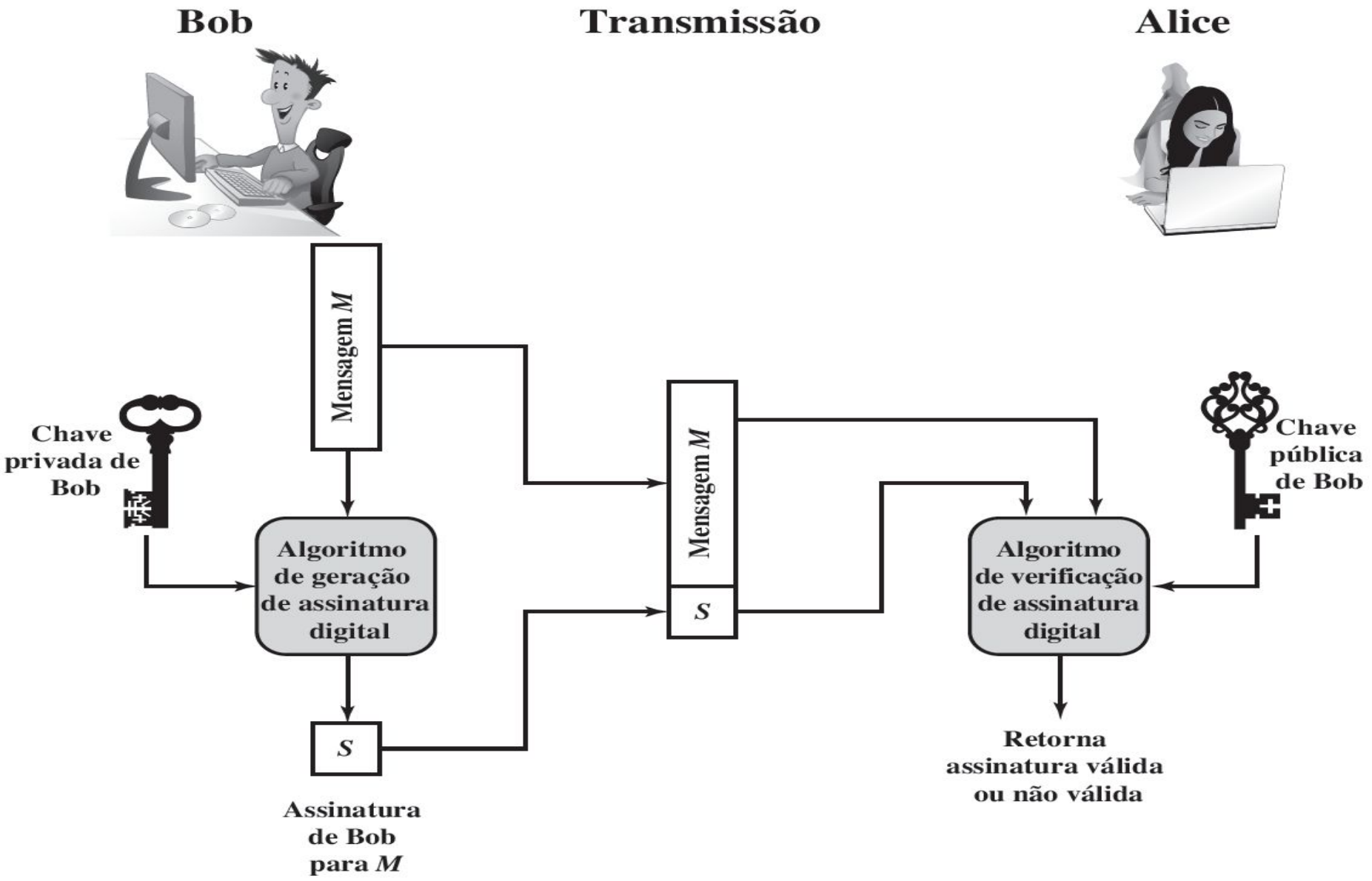
Assinaturas Digitais

- Similar à assinatura de uma pessoa, **visa garantir a autenticidade de uma mensagem.**

- **Protege duas partes** que trocam mensagens contra um terceiro qualquer.

- Precisa ter as seguintes características:
  - Verificar o autor, a data e a hora da assinatura;
  - Autenticar o conteúdo no momento da assinatura;
  - Ser verificável por terceiros, para resolver disputas.

Modelo Genérico



Requisitos de Assinatura Digital

Requisitos para uma assinatura digital:

- A assinatura precisa ser um padrão de bits que **depende da mensagem sendo assinada**.
- A assinatura precisa **usar alguma informação exclusiva do emissor**, para impedir falsificação e negação.
- É preciso ser relativamente **fácil produzir a assinatura digital**.

Requisitos de Assinatura Digital

Requisitos para uma assinatura digital:

- É preciso ser relativamente **fácil reconhecer e verificar a assinatura digital**.
- É preciso ser **computacionalmente inviável falsificar uma assinatura digital**, seja construindo uma nova mensagem para uma assinatura digital existente ou uma assinatura digital fraudulenta para determinada mensagem.
- É preciso ser **prático reter uma cópia da assinatura** digital em termos de armazenamento.

Algoritmo de Assinatura Digital do NIST

- O **DSA** (*Digital Signature Algorithm*) utiliza um algoritmo que é projetado para oferecer **apenas a função de assinatura digital**.

- Diferente do RSA, ele **não pode ser usado para encriptação ou troca de chave.**

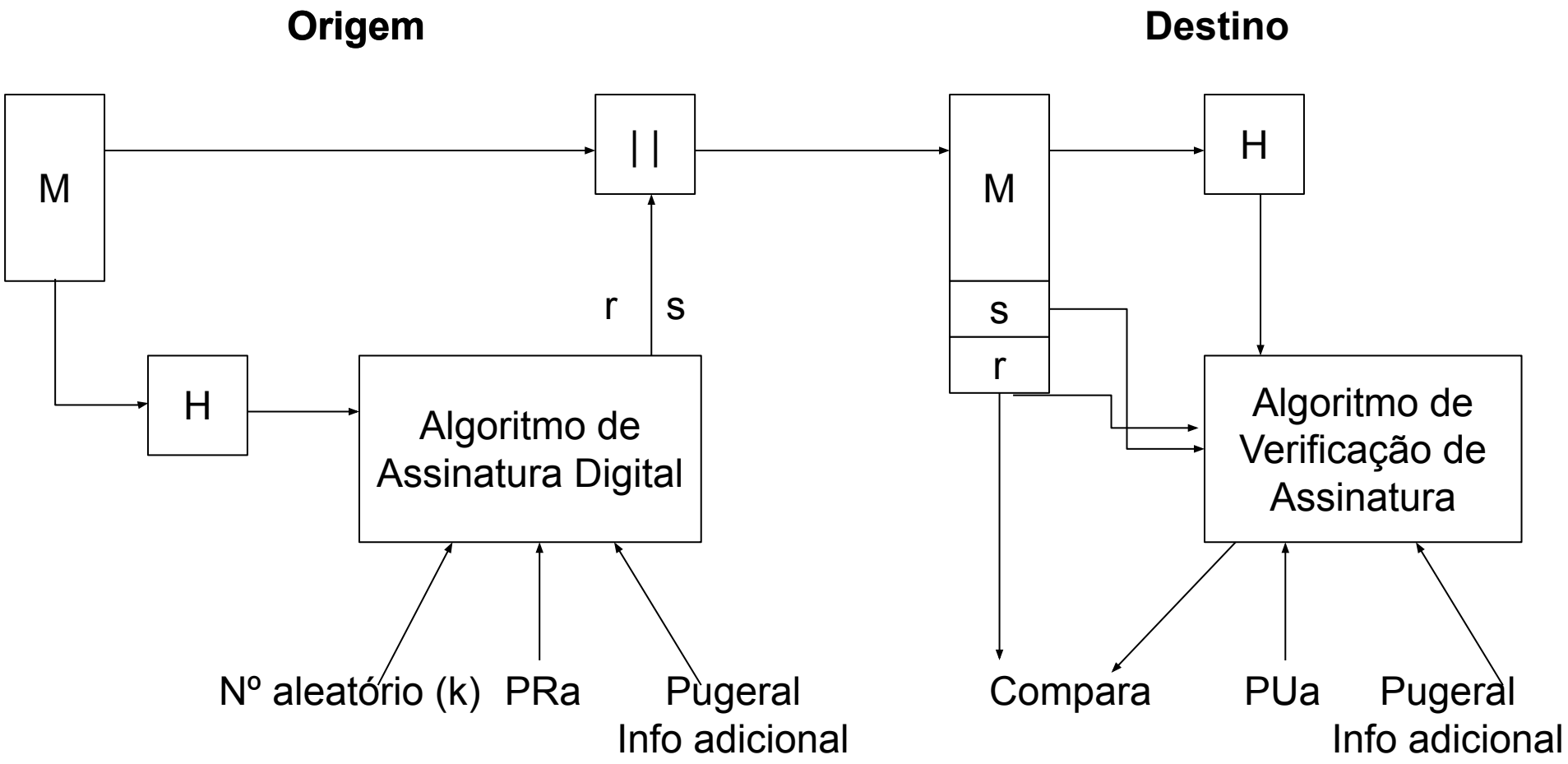
- Apesar disso, essa é uma **técnica de chave assimétrica**.

- A técnica do DSA **também usa uma função de hash.**

A função de assinatura é tal que somente o emissor, com conhecimento da chave privada, poderia ter produzido a assinatura válida.

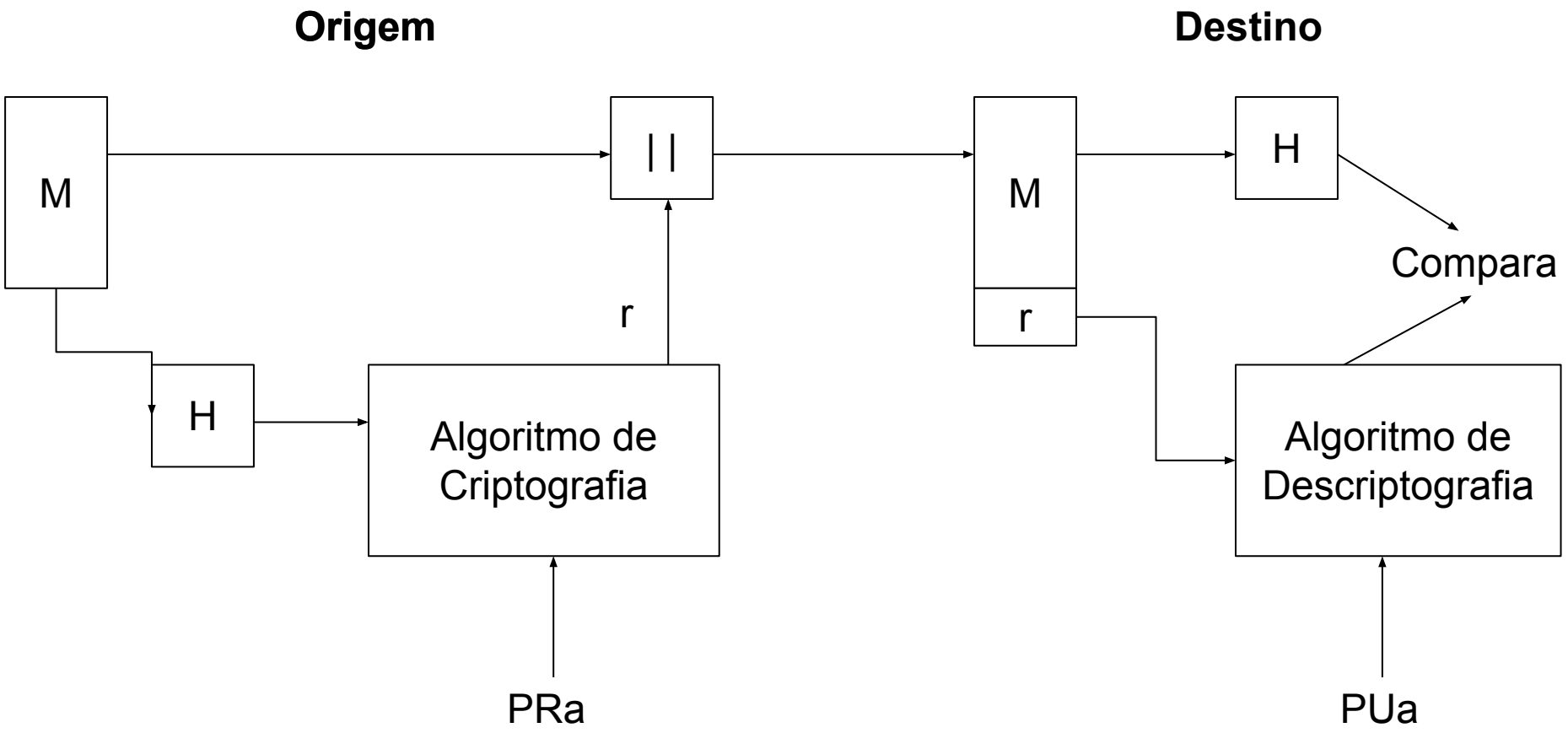
Algoritmo de Assinatura Digital do NIST

- Assinatura do DSA:



Algoritmo de Assinatura Digital do NIST

- Assinatura do RSA:



Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação simétrica.

- Para duas partes A e B, a distribuição de chave pode ser feita de várias maneiras:

1) A pode selecionar uma chave e entregá-la fisicamente a B.

Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação simétrica.

- Para duas partes A e B, a distribuição de chave pode ser feita de várias maneiras:

1) A pode selecionar uma chave e entregá-la fisicamente a B.

2) Um terceiro pode selecionar a chave e entregá-la fisicamente a A e B.

Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação simétrica.

- Para duas partes A e B, a distribuição de chave pode ser feita de várias maneiras:

1) A pode selecionar uma chave e entregá-la fisicamente a B.

2) Um terceiro pode selecionar a chave e entregá-la fisicamente a A e B.

3) Se A e B tiverem usado uma chave previamente e recentemente, uma parte pode transmitir a nova chave à outra, encriptada usando a chave antiga.

Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação simétrica.

- Para duas partes A e B, a distribuição de chave pode ser feita de várias maneiras:

1) A pode selecionar uma chave e entregá-la fisicamente a B.

2) Um terceiro pode selecionar a chave e entregá-la fisicamente a A e B.

3) Se A e B tiverem usado uma chave previamente e recentemente, uma parte pode transmitir a nova chave à outra, encriptada usando a chave antiga.

4) Se A e B tiverem uma conexão encriptada com um terceiro C, este pode entregar uma chave a A e B pelos links encriptados.

Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação simétrica.

- No quarto caso, **um Centro de Distribuição de Chaves (CDC) confiável é usado** para distribuir chaves a pares de usuários.
- O uso de um CDC é baseado no **uso de uma hierarquia de chaves.**
- No mínimo dois níveis de chaves são usados: **chave de sessão e chave mestra**.

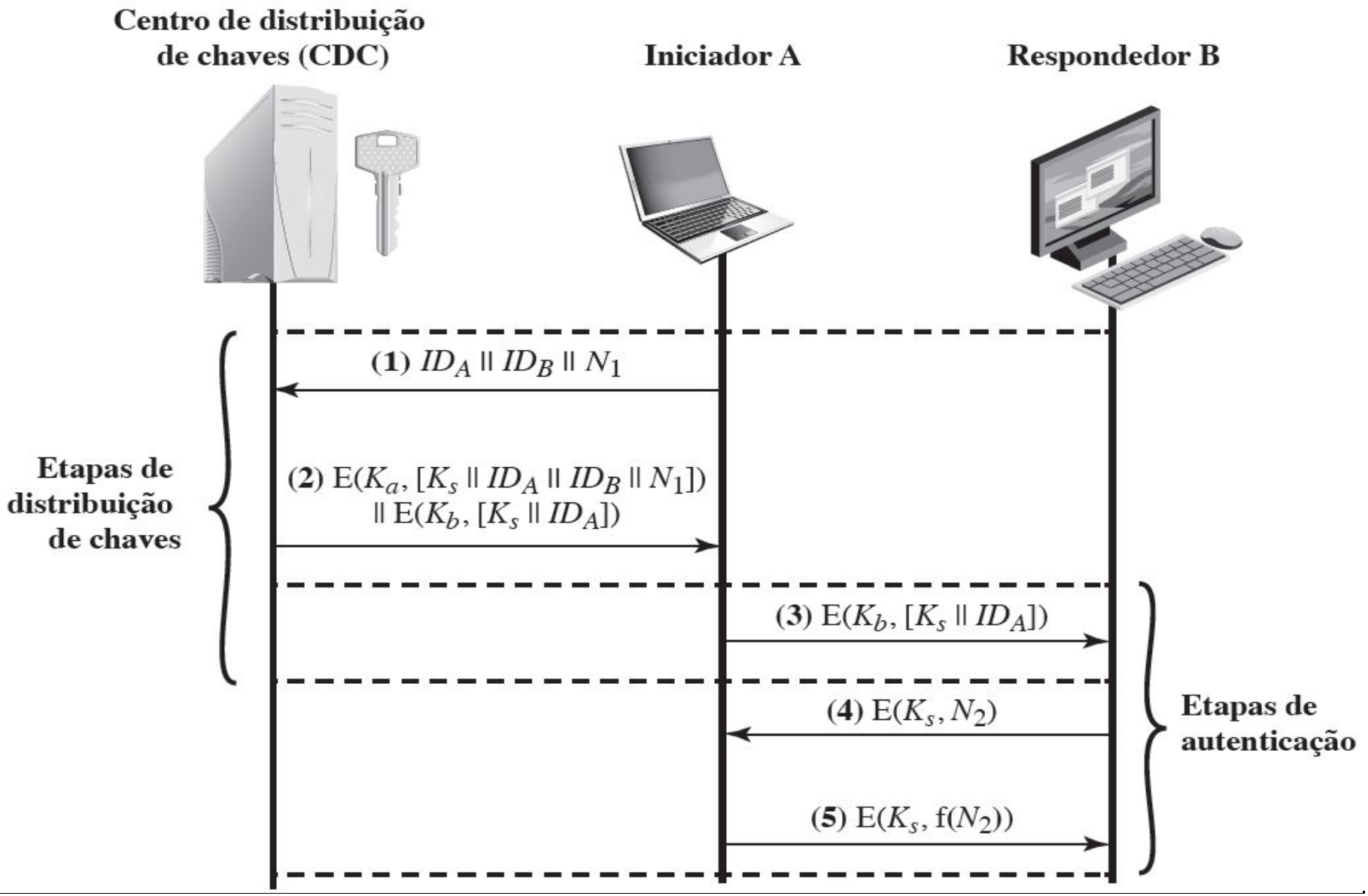
Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação simétrica.

- **Chave de sessão:** chave temporária, normalmente usada pela duração de uma conexão lógica e depois descartada.

- **Chave mestra:** chave exclusiva compartilhada entre o CDC e o sistema ou usuário final.

Distribuição de Chaves



Distribuição de Chaves

- A **emite uma solicitação ao CDC por uma chave de sessão** para proteger uma conexão lógica com B. A mensagem inclui IDa e IDb e um identificador exclusivo Nonce (tempo, nº aleatório, contador, etc).

- **O CDC responde com uma mensagem encriptada com Ka.** A mensagem contém: **a chave de sessão de uso único Ks, a mensagem de solicitação original, incluindo o nonce.**

- Além disso, **uma mensagem é destinada a B: chave de sessão de uso único Ks e o IDa** (ex: endereço de rede).

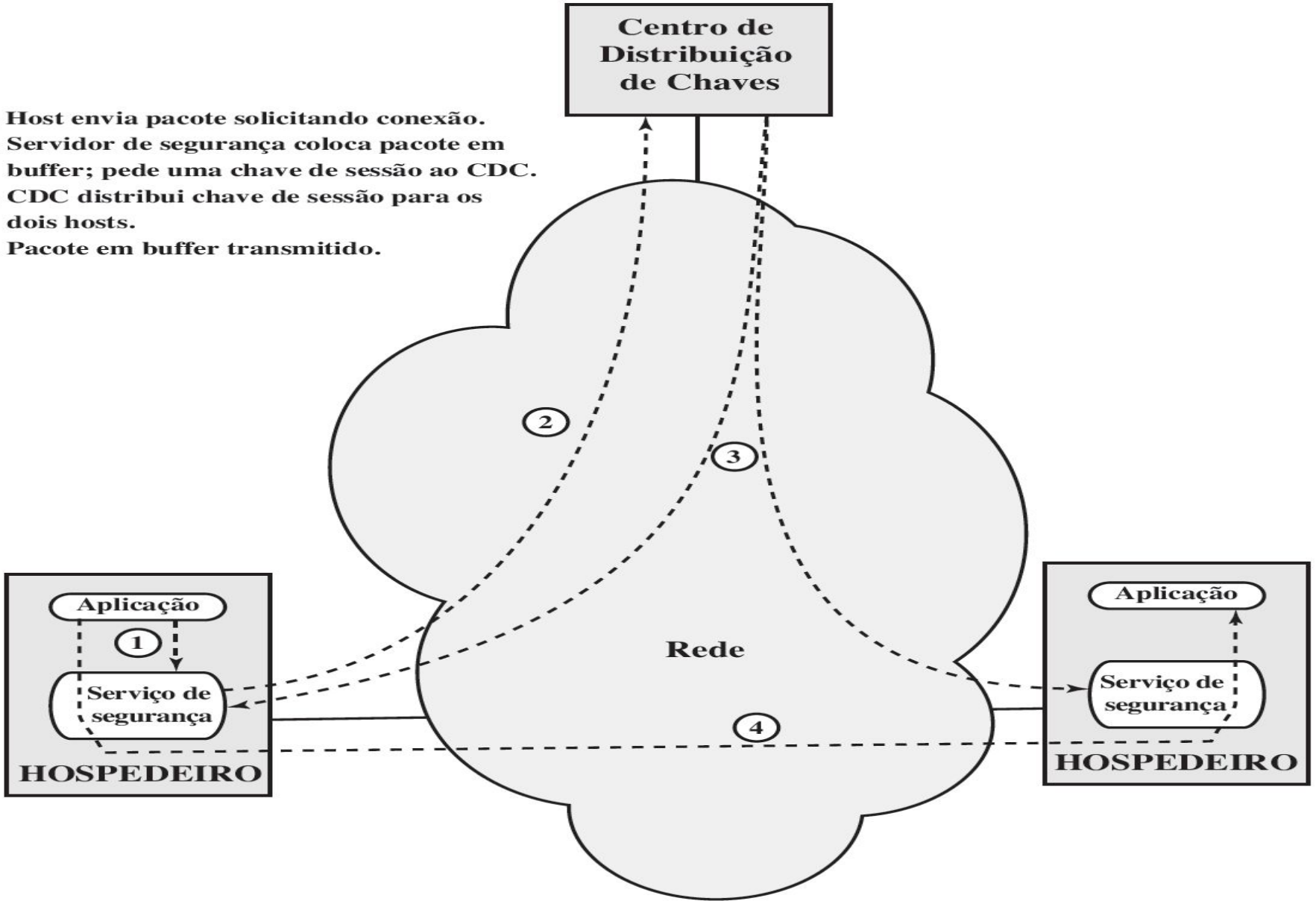
Distribuição de Chaves

- Não é necessário limitar a função de distribuição de chave a um único CDC.
- **Uma hierarquia de CDCs poderá ser estabelecida.**
- Esse esquema **limita o dano de um CDC defeituoso ou subvertido apenas à sua área local.**

Quanto mais frequentemente as chaves de sessão forem trocadas, mais seguras elas são → perda de desempenho.

Distribuição de Chaves

1. Host envia pacote solicitando conexão.
2. Servidor de segurança coloca pacote em buffer; pede uma chave de sessão ao CDC.
3. CDC distribui chave de sessão para os dois hosts.
4. Pacote em buffer transmitido.



Distribuição de Chaves

Além de separar chaves mestras de chaves de sessão, podemos querer definir **diferentes tipos de chaves de sessão com base no uso**, como:

- **Chave de encriptação de dados**, para comunicação geral por uma rede.
- **Chave de encriptação de PIN**, para números de identificação pessoal (PINs) usados em aplicações de transferência eletrônica de fundos e aplicações de ponto de venda.
- **Chave de encriptação de arquivo**, para encriptar arquivos armazenados em locais publicamente acessíveis.

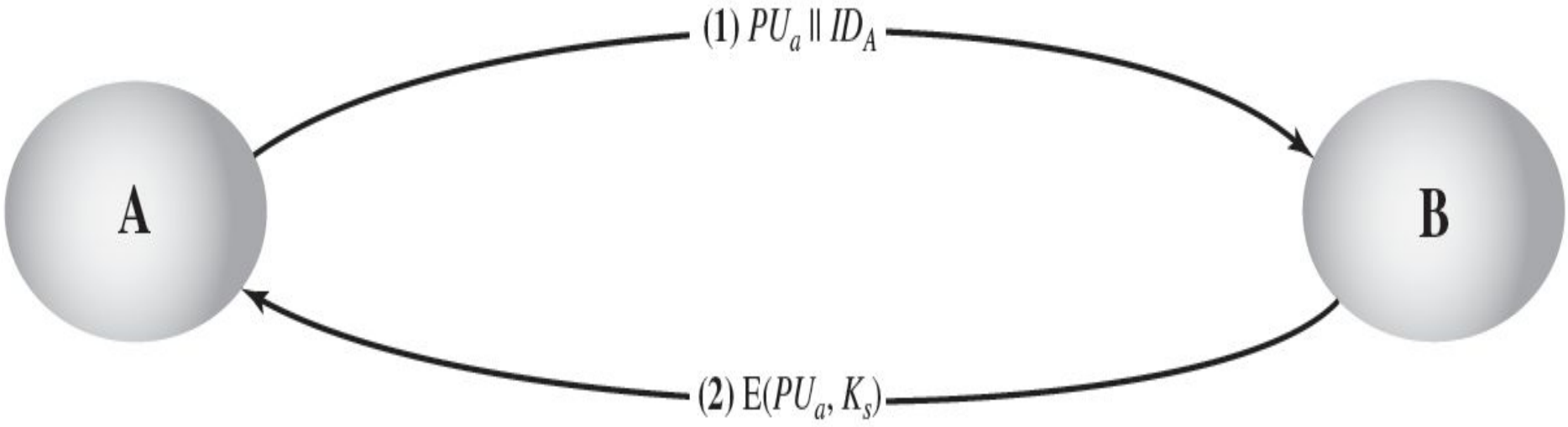
Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação assimétrica

- A gera par de chaves pública e privada e transmite uma mensagem para B contendo PUa e um IDa
- B gera um chave secreta Ks e a transmite a A, encriptada com chave pública de A
- A descriptografa para obter chave secreta utilizando sua chave privada
- A descarta PUa e PRa e B descarta PUa.

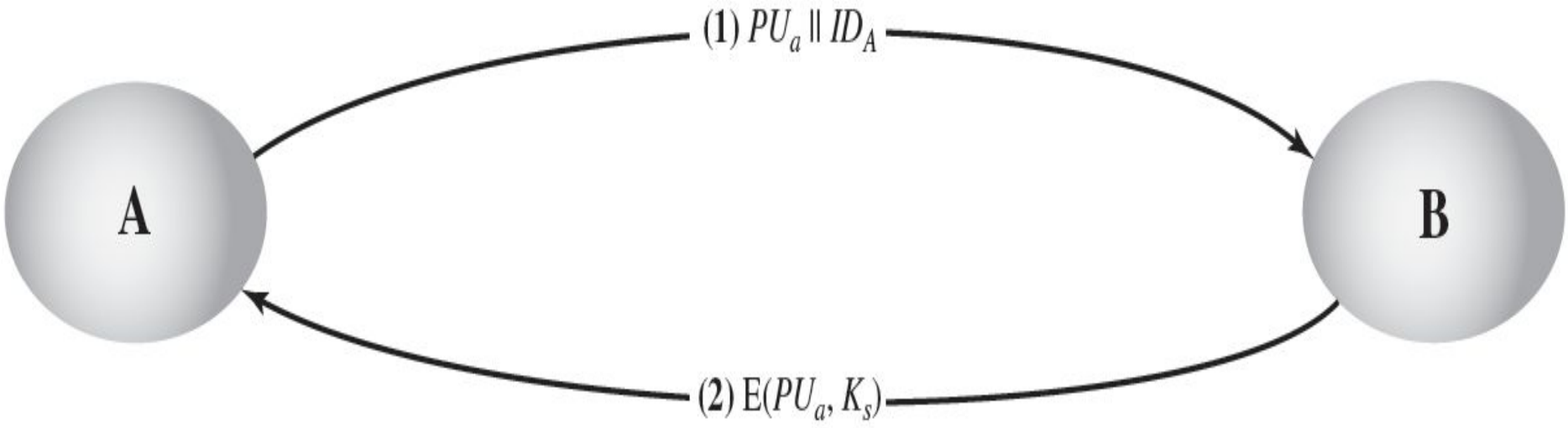
Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação assimétrica



Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação assimétrica



Quem garante que B é quem ele diz ser?

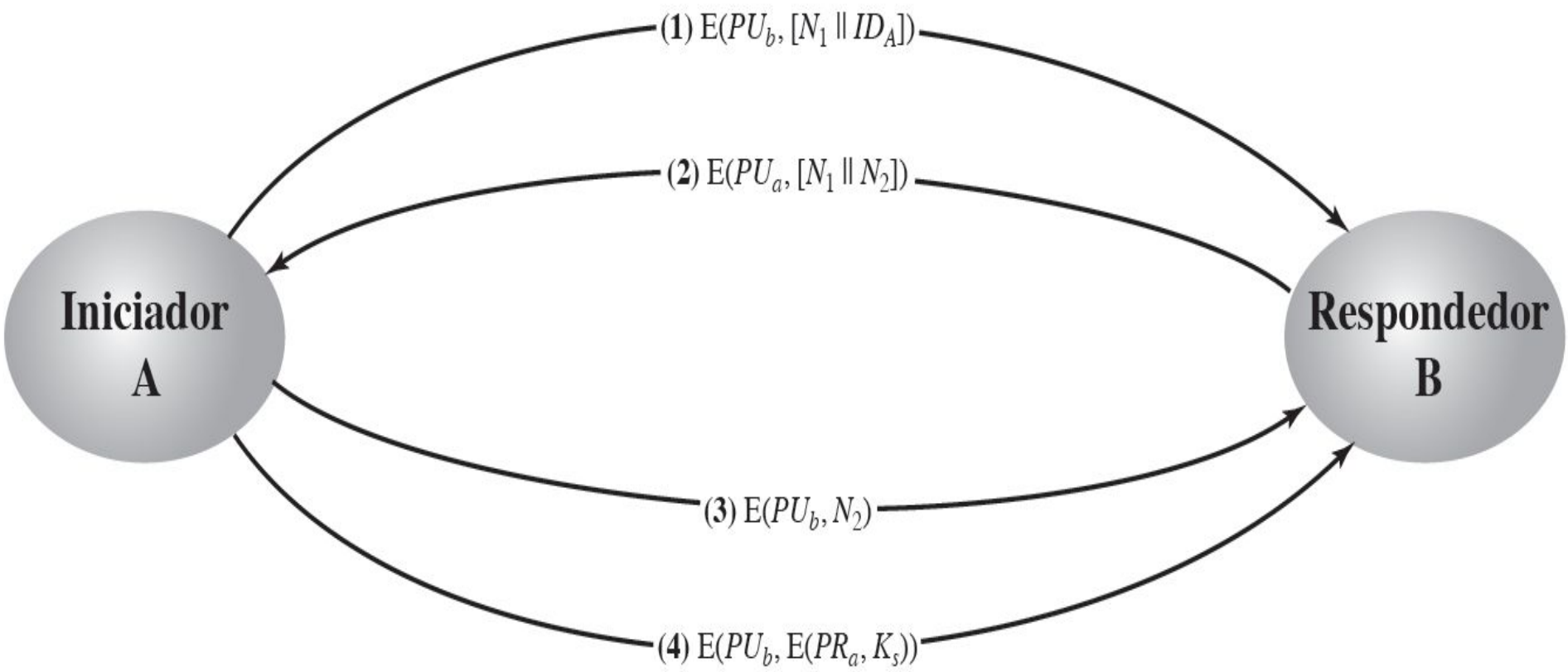
Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação assimétrica

- A usa chave pública de B para encriptar uma mensagem para B com o IDa e um nonce (N1) (identificador exclusivo de transação).
- B envia uma mensagem para A encriptada com PUa e contendo nonce (N1), além de um novo nonce (N2).
- A retorna N2 encriptado usado a chave pública de B.
- A seleciona uma chave secreta Ks e envia para B. i)criptografa Ks com sua chave privada; ii)criptografa o resultado com chave pública de B.
- B i)descriptografa usando a sua chave privada; ii)descriptografa usando chave pública de A.

Distribuição de Chaves

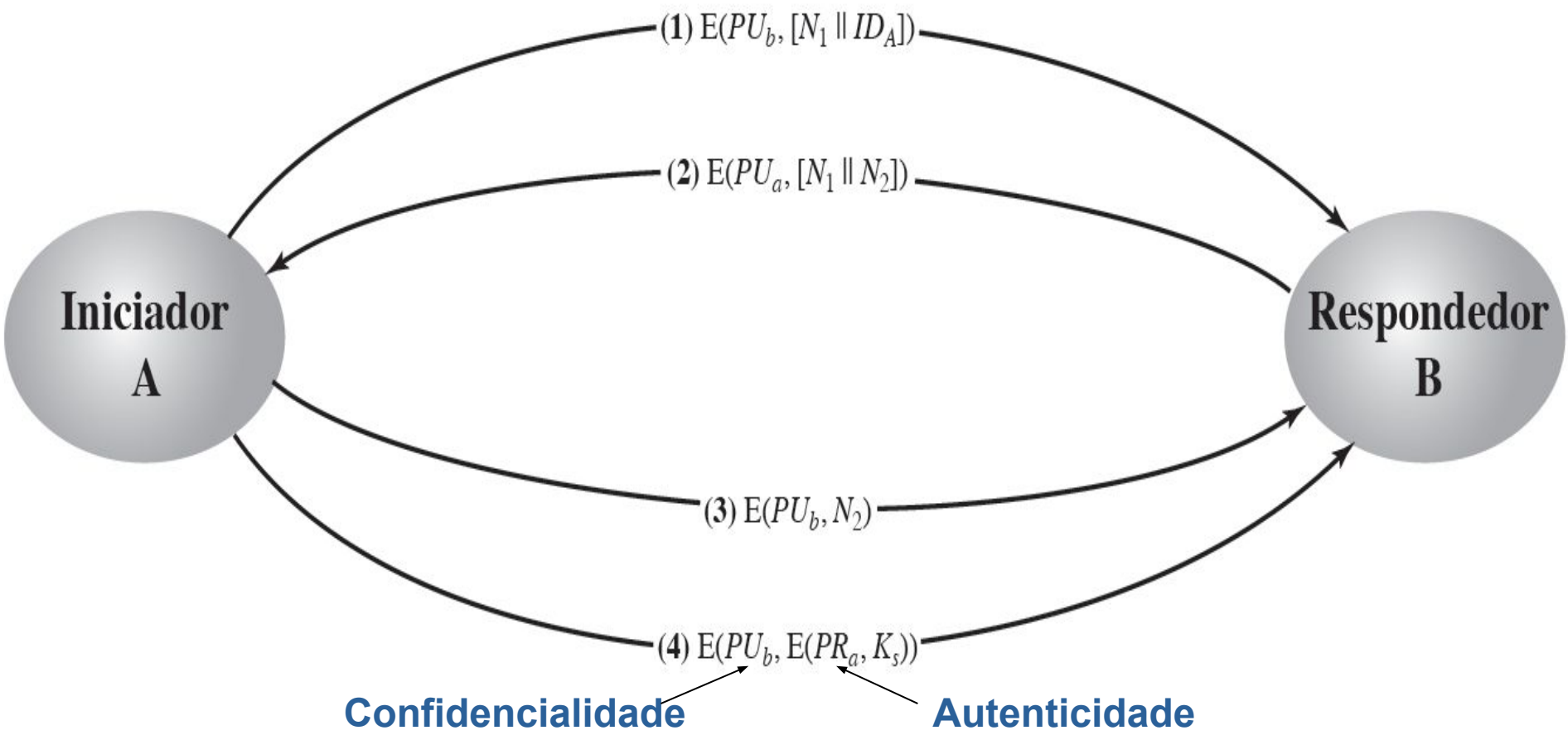
Distribuição de Chave Simétrica utilizando encriptação assimétrica



Garantiu confidencialidade e autenticidade?

Distribuição de Chaves

Distribuição de Chave Simétrica utilizando encriptação assimétrica



Distribuição de Chaves Públicas

Várias técnicas têm sido propostas para a distribuição de chaves públicas.

- **Anúncio público:** distribuição livre da chave pública.
- **Diretório disponível publicamente:** registro de chaves públicas.
- **Autoridade de chave pública:** semelhante a anterior, porém, autoridade conhece chave privada do emissor.
- **Certificados de chave pública:** autoridade certificadora (CA) confiável (ex: agência do governo) que atesta veracidade da mensagem.

Infraestrutura de Chaves Públicas

- A RFC 4949 define a infraestrutura de chave pública (**PKI – *Public Key Infrastructure***) como o **conjunto de *hardware*, *software*, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais com base na criptografia assimétrica.**

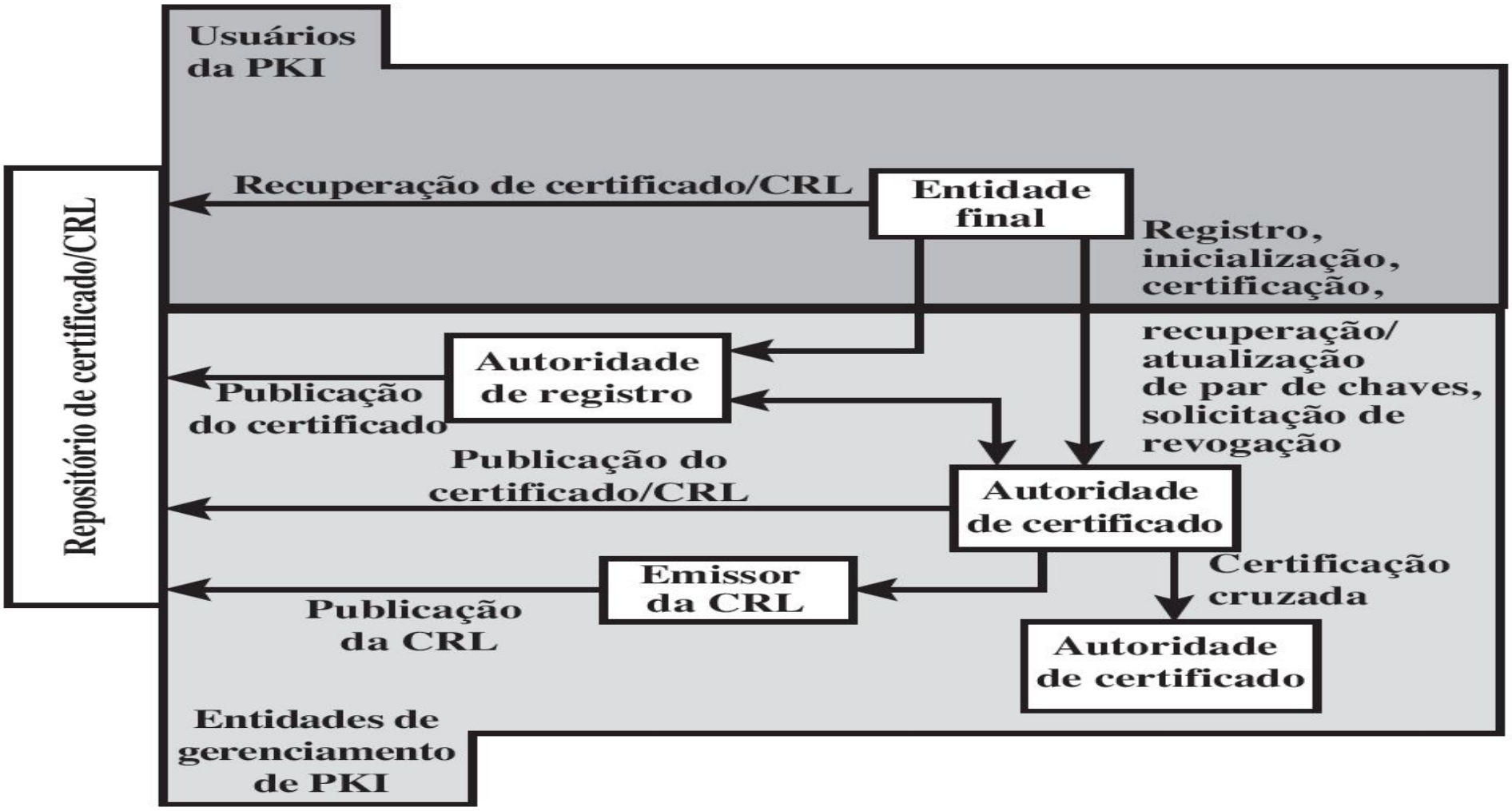
- O objetivo principal para desenvolver uma PKI é **permitir a aquisição segura, conveniente e eficiente de chaves públicas.**

Infraestrutura de Chaves Públicas

PKI identifica diversas funções de gerenciamento:

- **Registro:** registro do sistema final.
- **Inicialização:** o cliente precisa ser inicializado com informações importantes, como CAs confiáveis.
- **Certificação:** emissão de certificado de um usuário.
- **Recuperação do par de chaves:** restaurar par de chaves a partir de backup.
- **Atualização do par de chaves:** certificado expirou.
- **Solicitação de revogação:** situações anormais.
- **Certificação cruzada:** CAs trocam informações.

Infraestrutura de Chaves Públicas



Dúvidas?