INF-108

Segurança da Informação

ICP e Certificados Digitais

Prof. João Henrique Kleinschmidt

Criptografia de chave pública

- Oferece **criptografia** e também uma maneira de **identificar e autenticar** (através de assinatura) pessoas ou dispositivos.
- **Como obter uma chave pública** e numa comunicação **certificar-se de que essa chave tenha sido recebida da parte intencionada?**
- Com **Criptografia de Chave Pública** e **Assinatura Digital:** pessoas podem utilizar a chave pública de uma outra pessoa;
- Para **enviar uma mensagem** segura a uma pessoa, tomamos a **chave pública** dessa pessoa e **criamos um envelope digital.**
- Para **verificar a mensagem** de uma pessoa, adquire-se a **chave pública** dessa pessoa e **verifica-se a assinatura digital**.

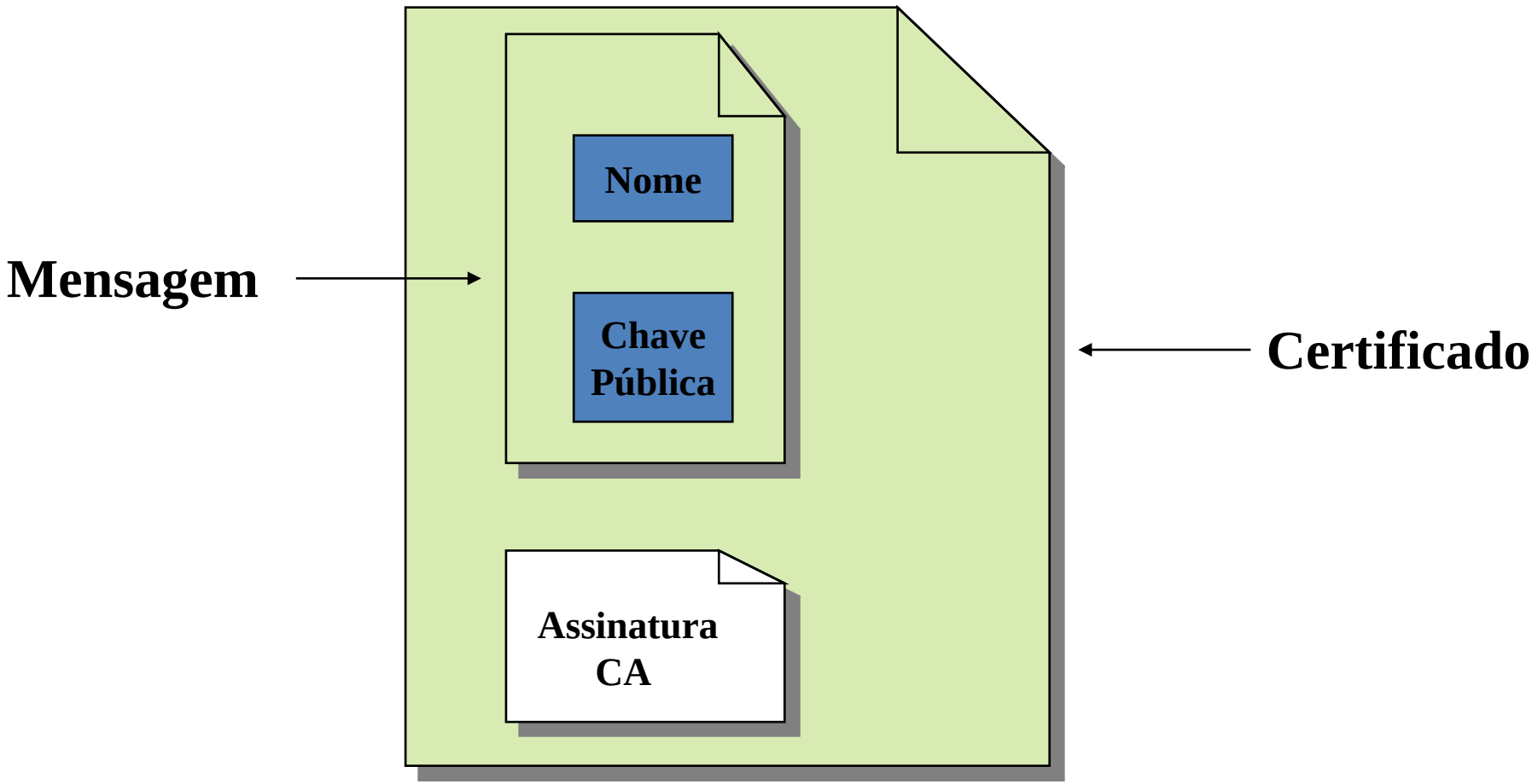
Exemplo de invasão 1

- Alice tem a chave pública de Bob.
  Ela é capaz de criar um envelope digital e se comunicar com Bob que é possuidor da chave privada relacionada à chave pública em poder de Alice.
- Mas se Eva, de alguma maneira, invade o computador de Alice e substitui a chave pública de Bob pela chave pública dela, quando Alice enviar o envelope digital, Eva será capaz de interceptá-lo e lê-lo. Bob não será capaz de abri-lo porque ele não tem a chave privada parceira da chave pública utilizada.

Exemplo de invasão 2

- Na empresa onde Alice e Bob trabalham tem um **diretório centralizado que armazena as chaves públicas** de todas as pessoas.
- Quando **Bob** quiser **verificar a assinatura** de Alice, ele vai ao diretório e localiza a chave pública de Alice.
- Mas se **Eva** tiver invadido esse diretório e **substituído a chave pública de Alice** pela **chave pública dela**, poderá enviar uma mensagem fraudulenta ao Bob com uma assinatura digital válida. Bob pensará que a mensagem veio de Alice, porque verificará a assinatura com o que ele pensa ser a chave pública de Alice.

Certificado digital



- Solução: certificado digital
- Usado para saber se uma chave pública pertence ou não a uma entidade.

Certificado digital

- Um certificado é produzido de tal maneira que o torna perceptível se um impostor pegou um certificado existente e substituiu a chave pública ou o nome.

- Qualquer pessoa ao examinar esse certificado saberá se está errado.
- Talvez o **nome** ou a **chave pública** esteja errado;
- Portanto, não se pode confiar nesse certificado, ou seja, o par (**nome**,**chave**).

Funcionamento

- **Alice** gera um par de chaves: (**chave privada**, **chave pública**).
- **Protege a chave privada**.
- Entra em contato com uma Autoridade de Certificação (CA), solicitando um certificado.
- CA verifica se **Alice** é a pessoa que diz ser, através de seus documentos pessoais.
- Alice usa sua **chave privada** para **assinar** a solicitação do certificado.
- CA sabe, então, que Alice tem acesso à chave privada parceira da chave pública apresentada, assim como sabe que a chave pública não foi substituída.

Funcionamento

- CA combina o **nome** Alice com a **chave pública** em uma mensagem e assina essa mensagem com sua chave privada (de CA).

- **Alice**, agora, **tem um certificado** e o **distribui**.

- Portanto, quando Bob coletar a **chave pública** de Alice, o que ele estará coletando será o **certificado** dela.

Funcionamento

- Suponha que **Eva** tente **substituir a chave pública de Alice** pela sua **própria chave** (troca da chave pública dentro do certificado).
- Ela pode localizar o arquivo da chave pública de Alice no laptop de Bob e substitui as chaves.
- **Bob**, antes de usar o certificado, utiliza a **chave pública de CA** para **verificar se o certificado é válido**.
- Pelo fato da mensagem no certificado ter sido alterada, **a assinatura não é verificada**.

Funcionamento

- Portanto, **Bob não criará um envelope digital usando essa chave pública** e Eve não será capaz de ler qualquer comunicação privada.

- Esse cenário assume que Bob tem a **chave pública de CA** e tem a certeza de que ninguém a substituiu com a chave de um impostor.

- Pelo fato dele, **Bob**, **poder extrair a chave do certificado** fornecido pela **CA**, ele sabe que tem a **verdadeira chave pública de CA**.

Infraestrutura de chave pública (ICP)

- PKI (*Public-Key Infrastructure*)

- Composta de:
- Usuários Finais
- Partes Verificadoras:
  aquelas que verificam a autenticidade de certificados de usuários finais.

- Chaves públicas devem ser fornecidas uns aos outros.

Infraestrutura de chave pública

- Solução apropriada: **certificados de chave pública**
- Fornecem um método para **distribuição de chaves públicas**.
- Um **certificado de chave pública** é um conjunto de dados à prova de falsificação que atesta a associação de uma chave pública a um usuário final.
- Para fornecer essa associação, uma **autoridade certificadora** (CA), confiável, confirma a identidade do usuário.
- CAs emitem **certificados digitais** para usuários finais, contendo **nome**, **chave pública** e outras informações que os identifiquem.
- Após serem assinados digitalmente, esses **certificados** podem ser transferidos e armazenados.

Infraestrutura de chave pública

- Tecnologia para utilizar PKI:

  (1) Padrão X.509

  (2) Componentes de PKI para criar, distribuir, gerenciar e revogar certificados.

Estrutura de certificado X.509

1. Versão
2. Número Serial
3. Identificador do algoritmo de assinatura
4. Nome do Emissor – nome distinto (DN) da CA que cria e emite.
5. Validade
6. Nome do **Sujeito** – nome DN da entidade final (**usuário** ou **empresa**).
7. Informação da Chave Pública do sujeito: (**valor** da chave, identificador do **algoritmo**, **parâmetros** do mesmo)
8. Identificador único do emissor: (**não recomendado** pela RFC2459)
9. Identificador único do sujeito: (**não recomendado** pela RFC2459)

Estrutura de certificado X.509

10. Extensões:

Identificador de Chave de Autoridade

Identificador de Chave de Sujeito

Utilização de chave

Utilização de Chave Estendida: Para uso de aplicativos e protocolos (TLS, SSL, ...), definindo as utilizações da chave pública para servidores de autenticação, autenticação de cliente, registro de data/hora e outros.

Ponto de Distribuição de CRL

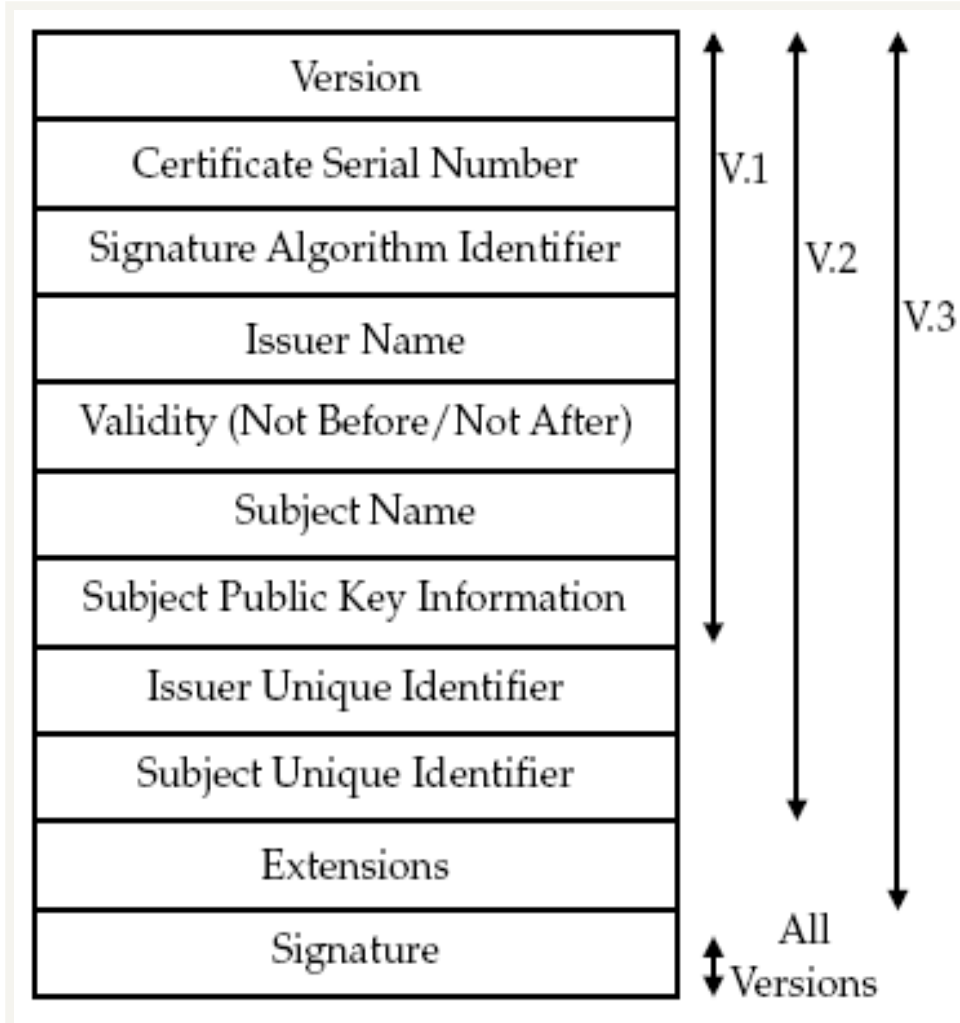
Período de Uso da Chave Privada: não recomendado pela RFC

Políticas de Certificado

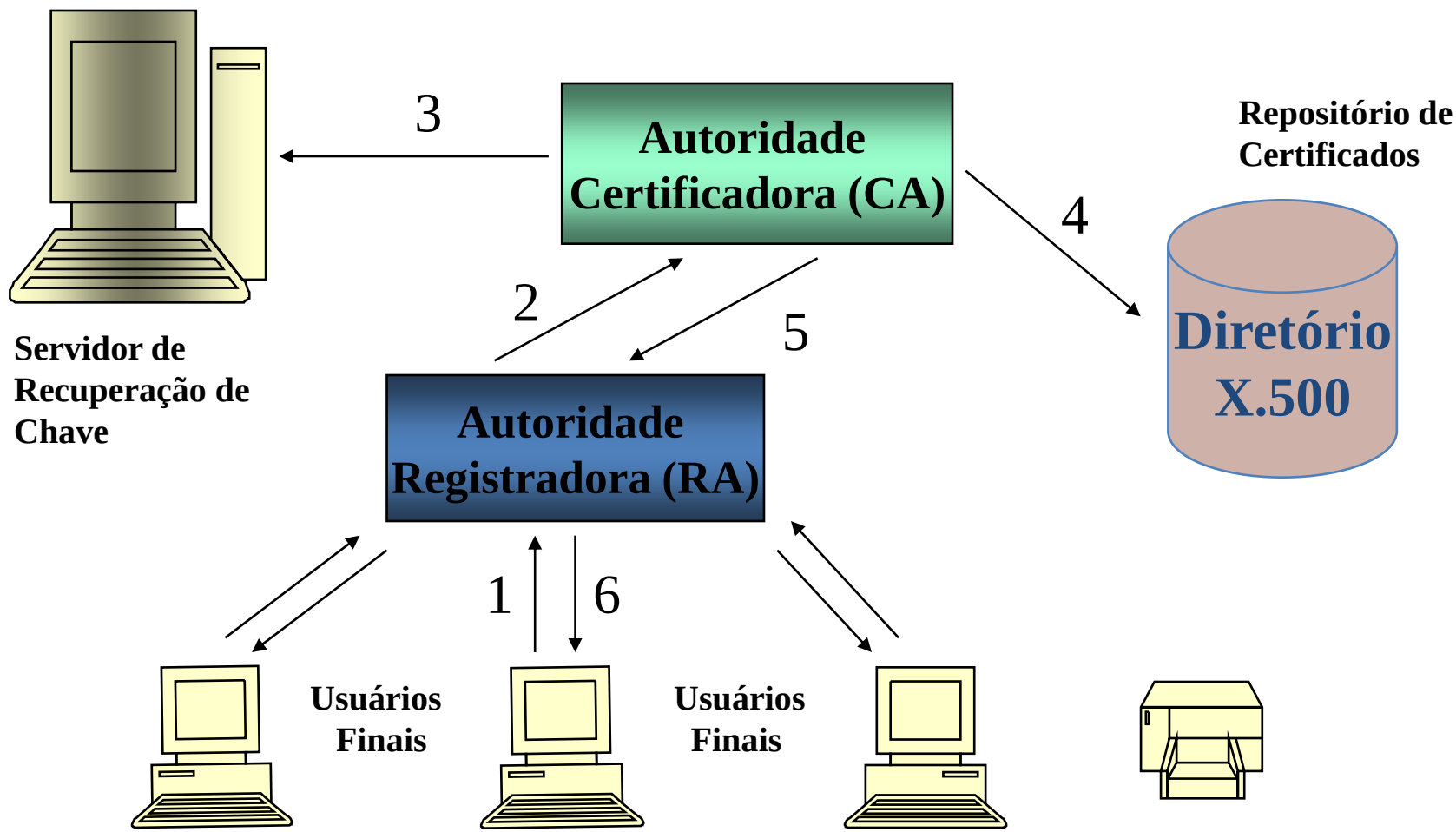
Mapeamentos de políticas: Quando o sujeito de certificado for uma CA.

- **Nome alternativo do sujeito**
- **Nome alternativo do emissor**
- **Atributos do diretório do sujeito**: (**não recomendado** pela RFC 2459)
- **Restrições básicas**: Se o sujeito pode agir como uma CA.
- **Restrições de nomes**: Apenas dentro de CAs. Especifica o espaço de nomes de sujeito.
- **Restrições de diretiva**: Apenas dentro de CAs. Validação de caminho de política.

Estrutura do certificado X.509



Componentes de uma ICP



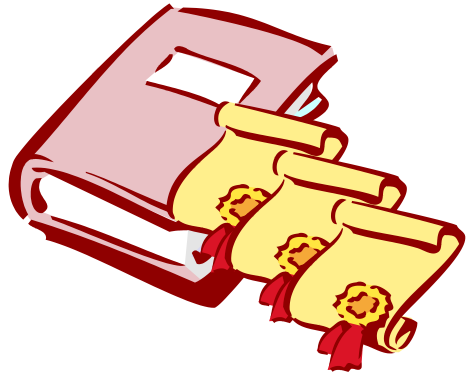
Autoridade Certificadora

- O aspecto principal de uma CA é o da confiança
- Tem a função de garantir a associação de um portador (pessoa ou entidade) com seu par de chaves
- Emite os certificados digitais a partir de uma política estabelecida, que define como deve ser verificada a identidade do portador, e quais devem ser as regras e condições de segurança da própria CA.

Autoridade Registradora

- Autoridades Registradoras implementam a interface entre os usuários e a Autoridade Certificadora
- A AR encarrega-se de receber as requisições de emissão ou de revogação de certificado do usuário, confirmar a identidade destes usuários e a validade de sua requisição
- Entrega os certificados assinados pela AC aos seus respectivos solicitantes

Diretório



- Um **diretório** é um arquivo, frequentemente de um tipo especial, que provê um mapeamento de **nomes-texto** para **identificadores internos de arquivo**.

- **Diretórios** podem incluir **nomes de outros diretórios**, correspondendo ao esquema familiar hierárquico de **nomeação de arquivos** e **nomes de caminhos** (*pathnames*) para arquivos usados em sistemas operacionais.

Servidor de Recuperação de Chave

- Num ambiente ICP, alguns usuários finais perderão suas chaves privadas.
- O CA deve então revogar o certificado, gerar um novo par de chaves e um novo certificado.
- Solução: servidor de recuperação que faça o backup de chaves privadas

Protocolos de Gerenciamento

- Comunicação on-line com os usuários finais e o gerenciamento dentro de uma PKI.
- Entre RA e um usuário final.
- Entre duas CAs.
- **Funções**

  - Inicialização
  - Registro
  - Certificação
  - Recuperação de chave
  - Atualização de chave
  - Revogação
  - Certificação cruzada

Protocolos Operacionais

- Permitem a **transferência de certificados** e das **informações de status de revogação**, entre diretórios, usuários finais e parte verificadoras.
- X.509 não especifica nenhum único protocolo operacional para uso dentro de um domínio de ICP.
- Protocolos usados:

  - HTTP,
  - FTP,
  - e-mail
  - LDAP - *Lightweight Diretory Access Protocol*

Registro de Certificados

- **Usuários finais se registram na CA ou na RA**, via Internet, utilizando um navegador da Web.

- É nesse ponto que usuário final e CA estabelecem uma **relação de confiança**.

- Geralmente a CA pede comprovação de rendimentos e prova de identidade por meio de contatos em pessoa.

Revogação de Certificados

- Certificados são criados para serem usados pelo tempo de vida indicado no campo de validade.
- Em alguns casos não deverá ser mais utilizado. Exemplo: chave privada comprometida, CA cometeu um equívoco ou possuidor da chave não trabalha mais numa empresa.
- CAs precisam de uma maneira de revogar um certificado ainda em vigor e notificar as partes verificadoras sobre a revogação.
- Método comum: Lista de Revogação de Certificado (CRL)

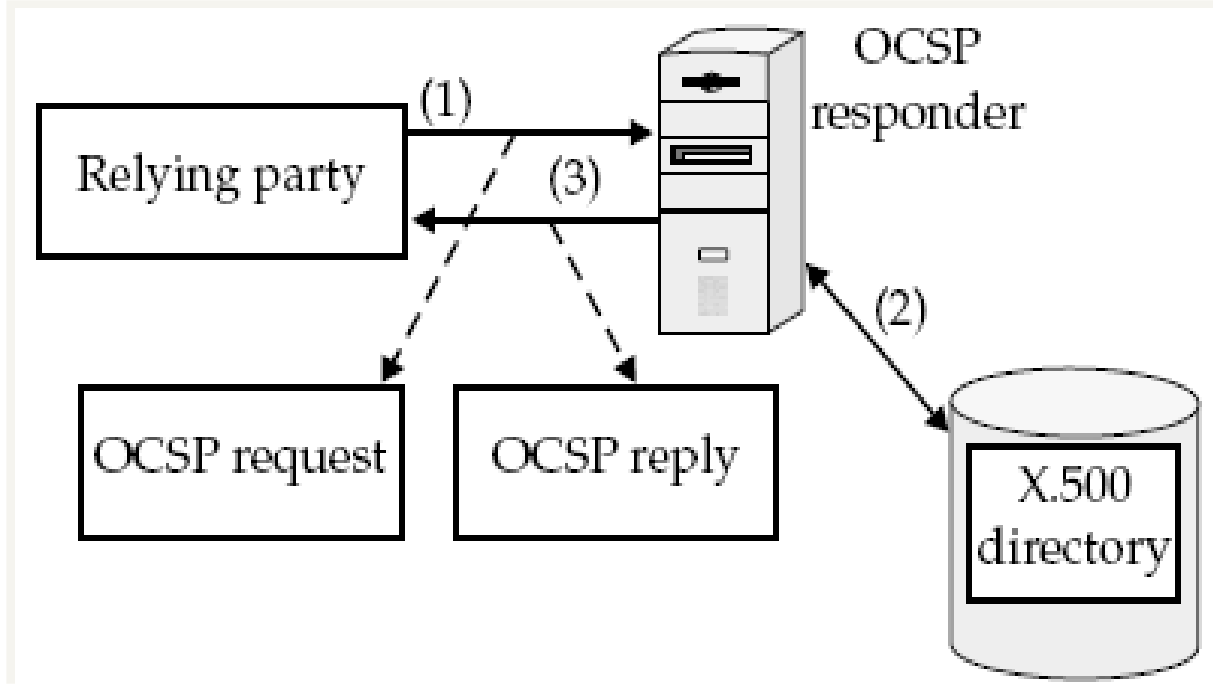
  - Estrutura de dados assinada contendo uma lista dos certificados revogados

Estrutura de uma CRL

Version
Signature Algorithm Identifier
Issuer Name
This Update (Date/Time)
Next Update (Date/Time)
User Certificate Serial Number / Revocation Date
CRL Entry Extensions
. . .
User Certificate Serial Number / Revocation Date
CRL Entry Extensions
CRL Extensions
Signature

Protocolo on-line do status de certificado (OCSP)

- Dependendo do tamanho da população da ICP, a carga de trabalho associada às CRLs pode tornar-se muito pesada.
- O protocolo OCSP pode ser utilizado por uma **parte verificadora** para **verificar a validade** de um **certificado digital**, no momento de uma transação (tempo real).

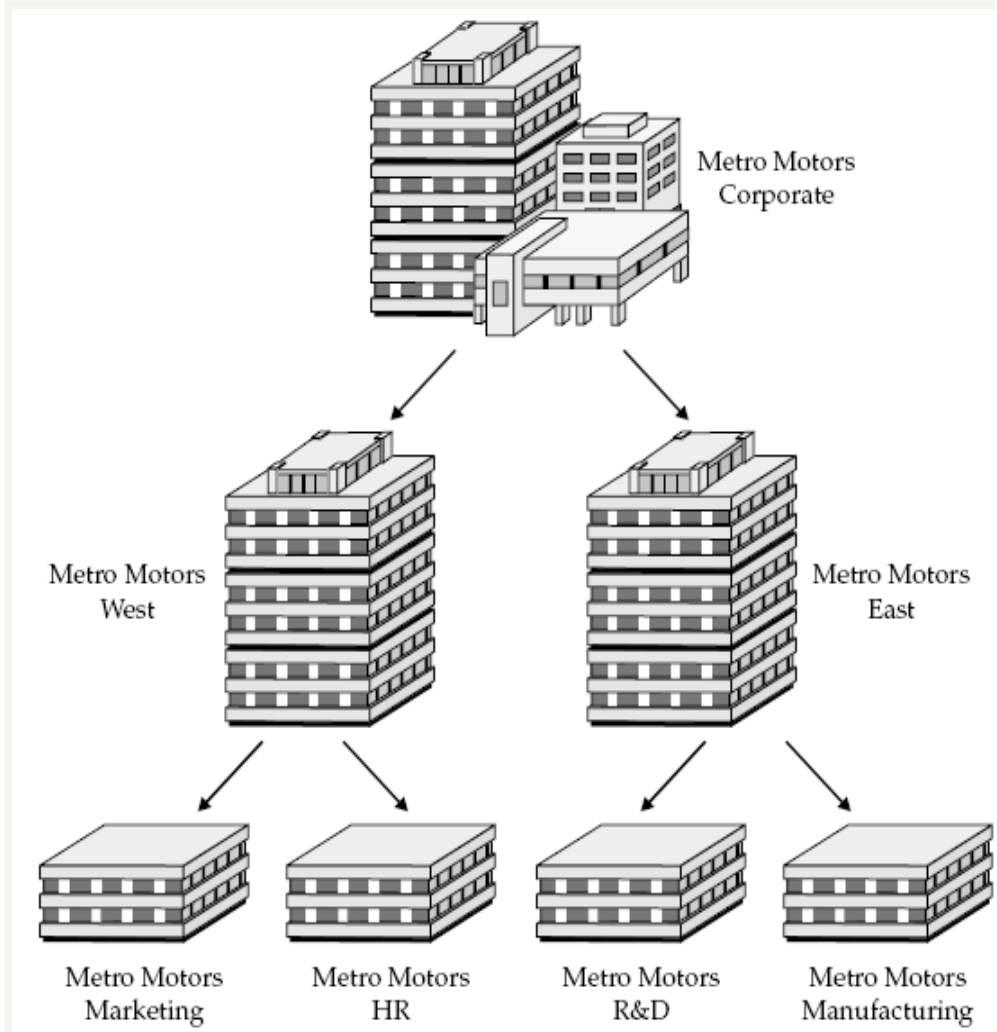


Protocolo on-line do status de certificado (OCSP)

- Uma parte verificadora pode consultar um servidor para determinar o status de um certificado.
- O servidor OCSP fornece uma resposta assinada digitalmente para cada um dos certificados cujas validades são solicitadas.
- **Respostas** OCSP consistem em:

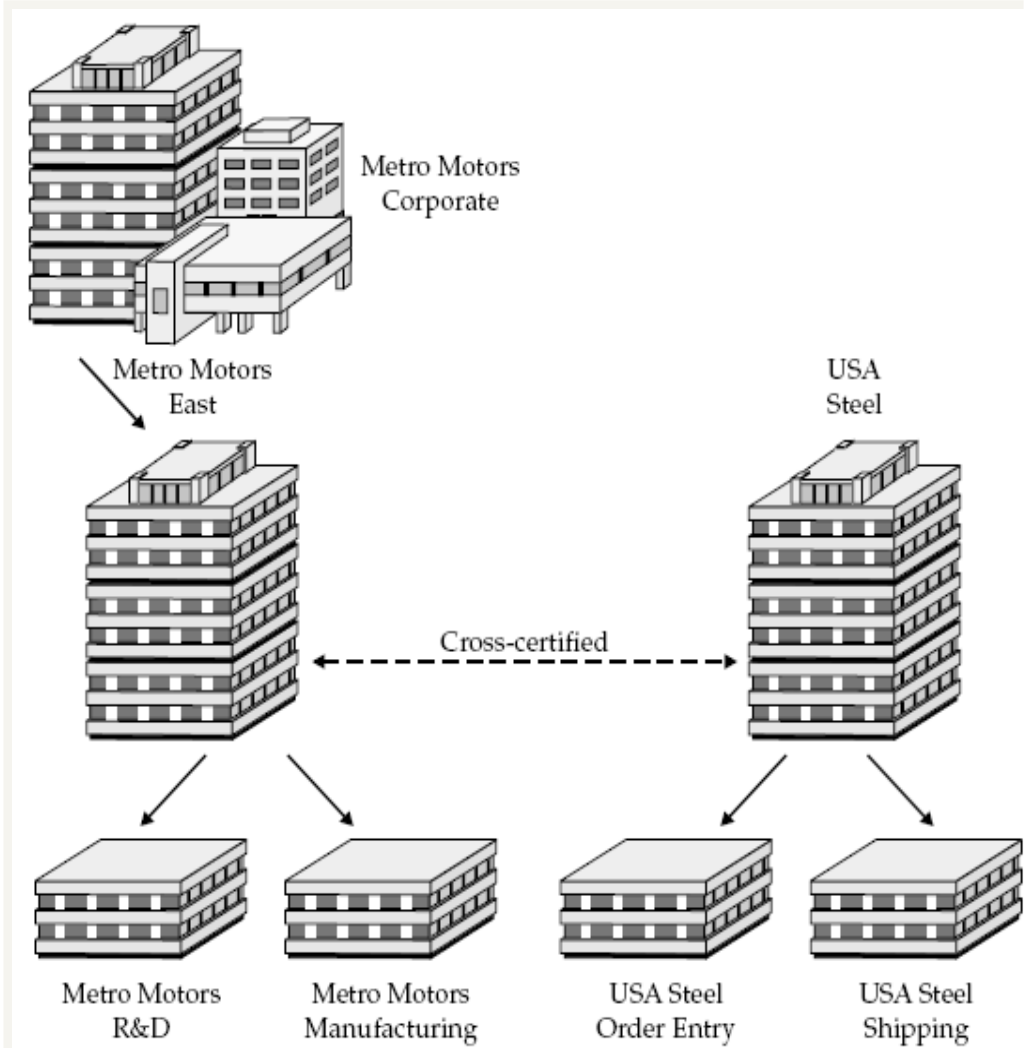
  - identificador de certificado,
  - valor do *status*
    (*good*, *revoke*, *unknown*),
  - intervalo de validade,
  - tempo de revogação,
  - razão da revogação.

Modelos de confiança



Hierarquias
de certificado

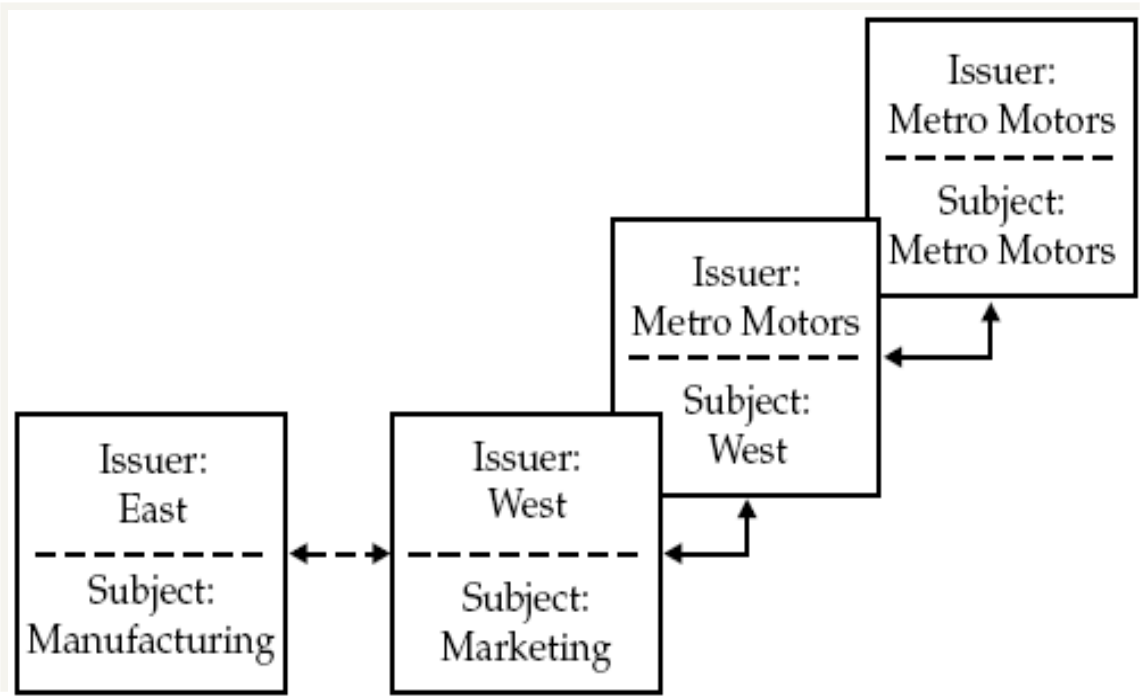
Modelos de confiança



Certificação cruzada

Cadeia de certificados X.509

- Utilizado para verificar a associação entre uma entidade e sua chave pública



Gerando Pares de Chaves

- **Primeira alternativa:**
- O usuário final gera um par de chaves (privada e pública) no seu sistema e fornece a chave pública na forma de um padrão de solicitação de assinatura de certificado de PKCS #10.
- **Segunda alternativa:**
- CA ou RA gera um par de chaves (privada e pública) em favor do usuário final.
- **Terceira alternativa:**
- Uso de múltiplos pares de chaves.
- Usuários finais podem ter mais de um certificado para diferentes propósitos.
- O usuário final gera as chaves para fornecer não-repúdio e a CA fornece as chaves de criptografia.

Atualizando Pares de Chaves

- Depois que o certificado expirou, a CA pode emitir novo certificado baseado no par de chaves originais ou gerar um novo par de chaves.
- Podem ser atualizadas de duas maneiras:
- Manual – usuário solicita atualização
- Automática – sistema verifica se certificado precisa de atualização

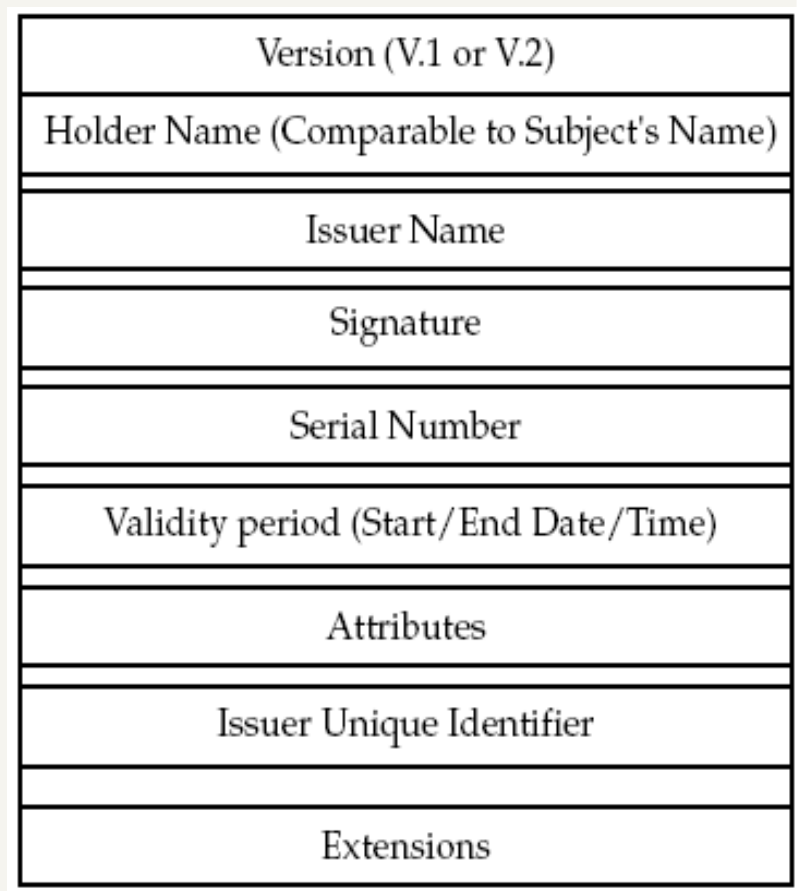
Mantendo histórico dos pares de chaves

- Fornece uma maneira para arquivar chaves e certificados para uma posterior utilização.

- O histórico é utilizado para recuperar assinaturas de certificados expirados ou arquivos criptografados com chaves que não são mais utilizadas.

Certificados de Atributo

- Utilizados para associar uma entidade a um conjunto de atributos.
- Aplicações: fornecer acesso remoto aos recursos de rede ou acesso físico em edifícios e instalações.

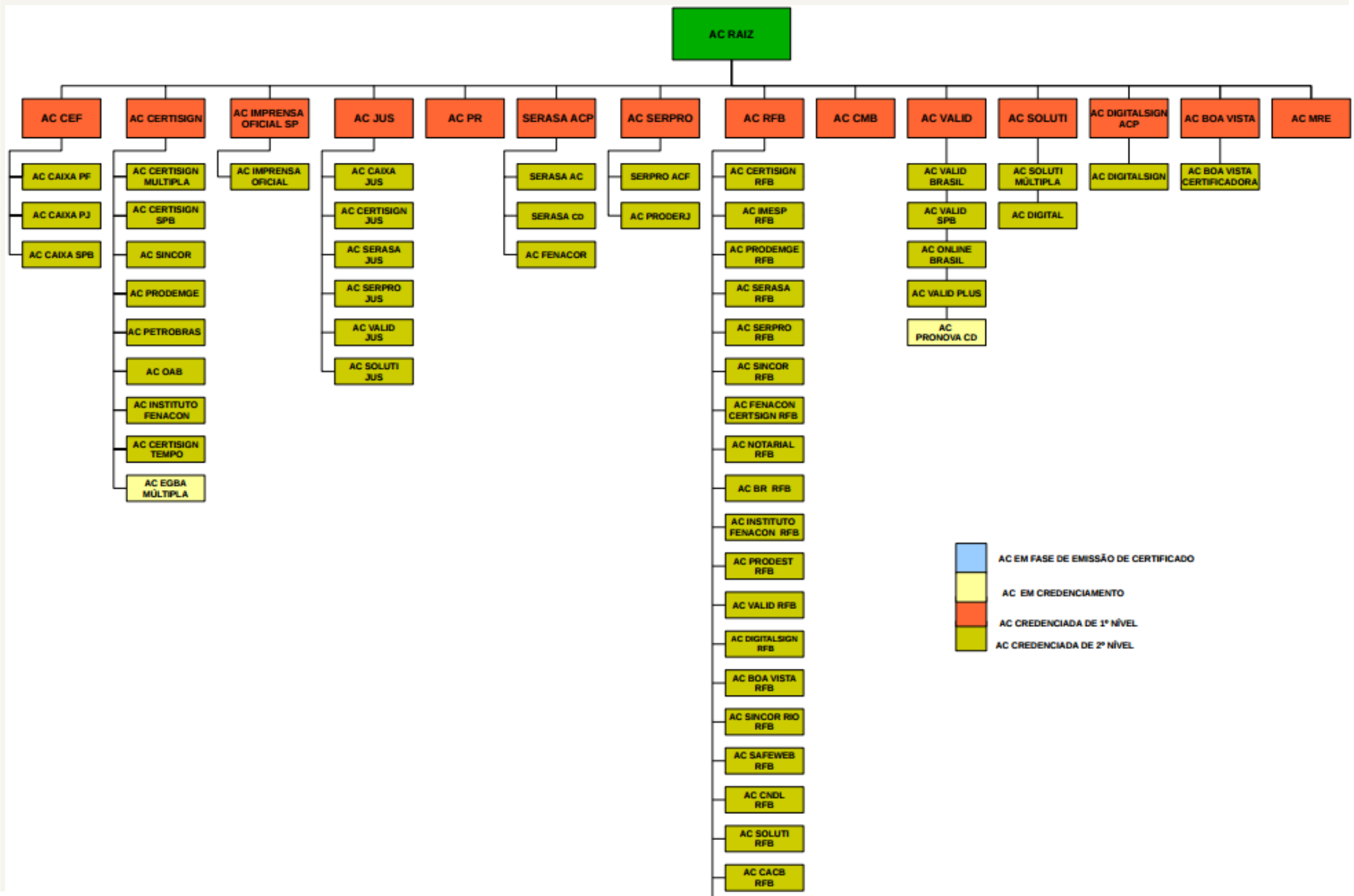


ICP - Brasil

- O **Instituto Nacional de Tecnologia da Informação - ITI** é uma autarquia federal vinculada à Casa Civil da Presidência da República.

- O ITI é a Autoridade Certificadora Raiz - **AC Raiz** da Infra-Estrutura de Chaves Públicas Brasileira - **ICP-Brasil**.

Estrutura da ICP Brasil



ICP

- Qualquer instituição pode criar uma ICP, independente de seu porte.

- Por exemplo, se uma empresa criou uma política de uso de certificados digitais para a troca de informações entre a matriz e sua filiais, não vai ser necessário pedir tais certificados a uma AC controlada pela ICP-Brasil.

- A própria empresa pode criar sua ICP e fazer com que um departamento das filiais atue como AC ou AR, solicitando ou emitindo certificados para seus funcionários.

Como obter um certificado digital

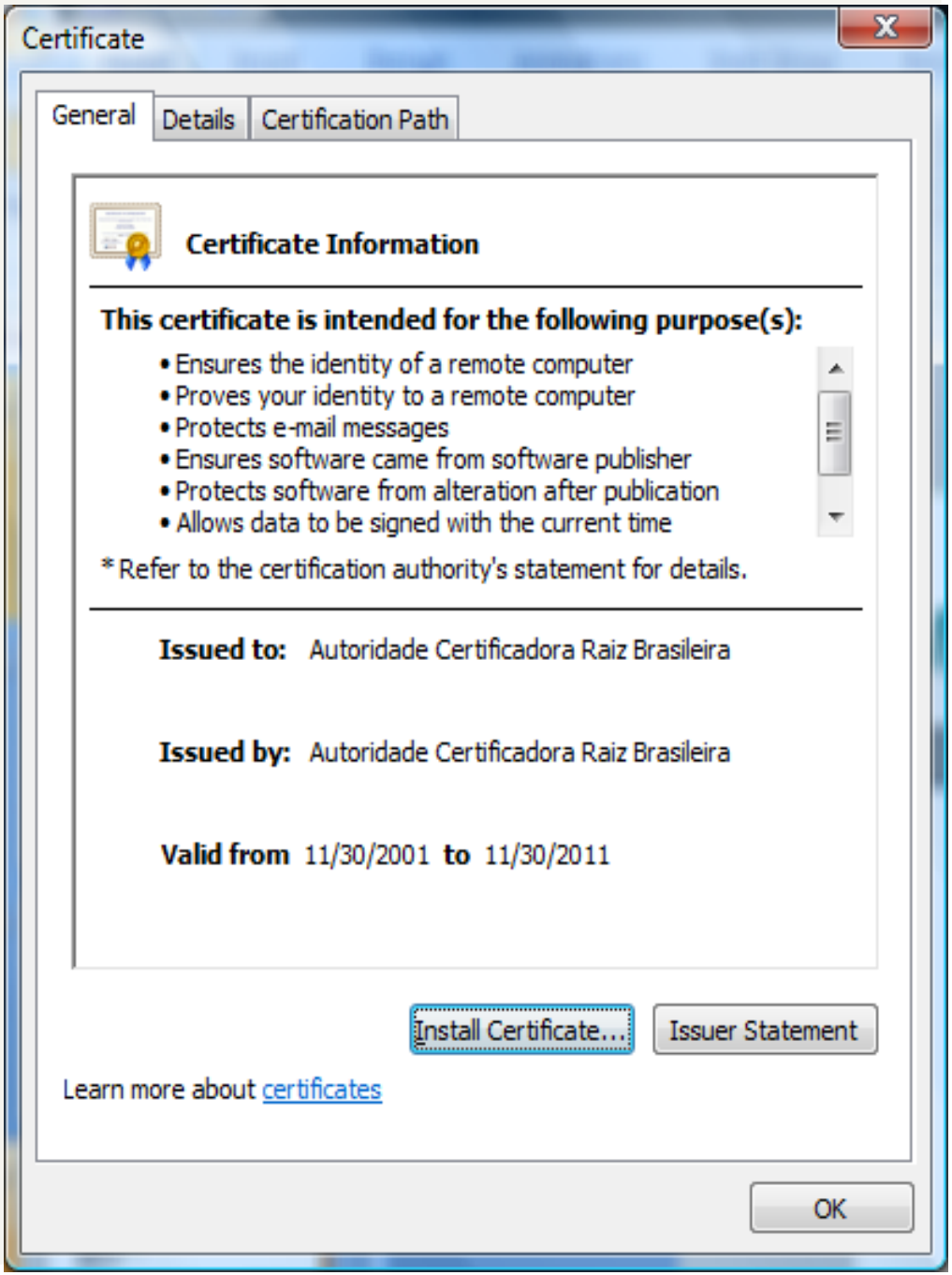
1) Acesse o site da Autoridade Certificadora;
2) Escolha o tipo de Certificado que deseja e preencha o formulário disponibilizado;
3) Realize o pagamento do Certificado;
4) Compareça a uma Autoridade de Registro indicada pela Autoridade Certificadora para validação de seus documentos.

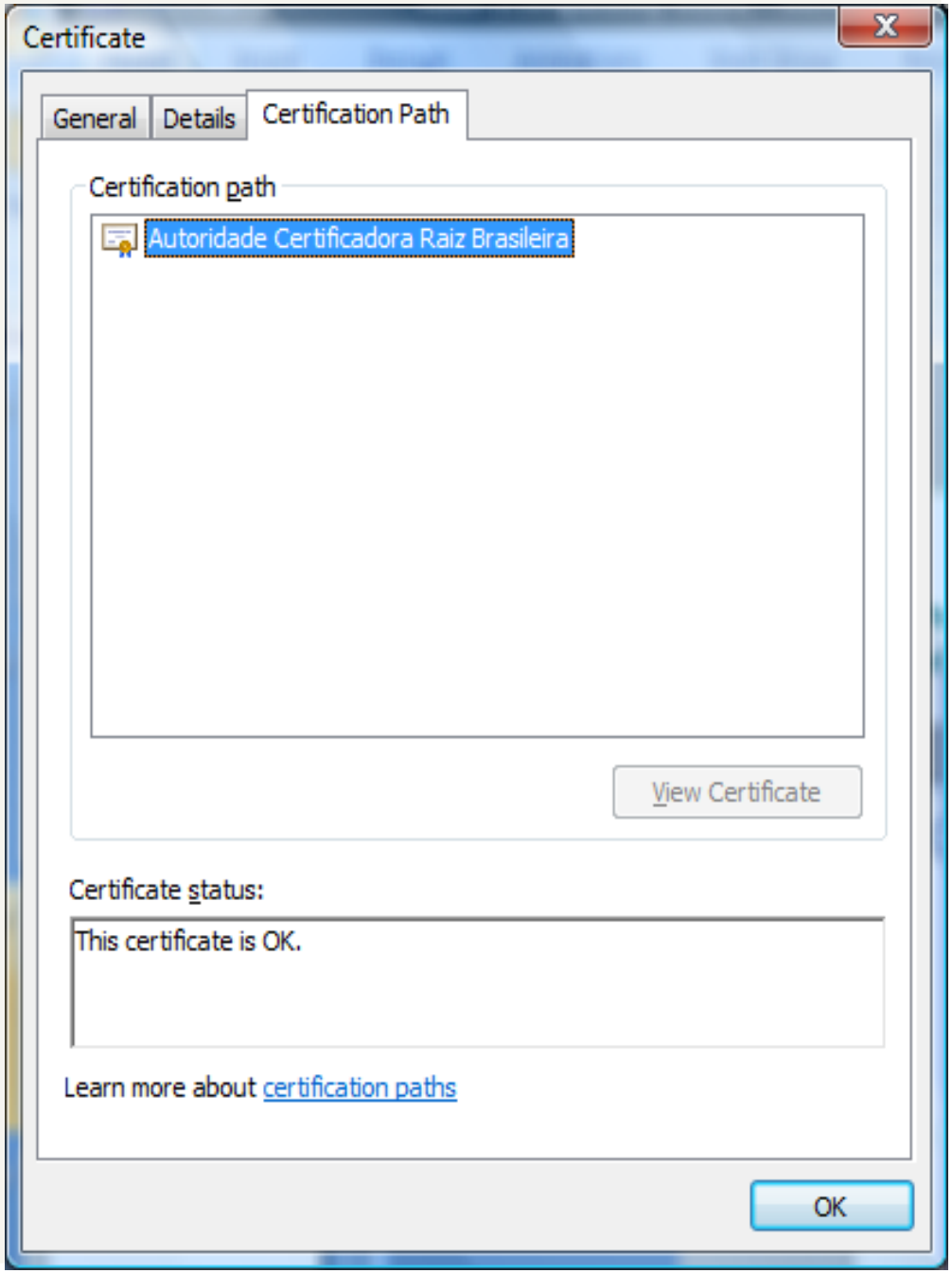
Algumas autoridades certificadoras subordinadas à ICP-Brasil e que comercializam certificados digitais:

- Caixa Econômica Federal
- Certisign
- SERASA
- SERPRO

Tipos de certificados ICP-Brasil

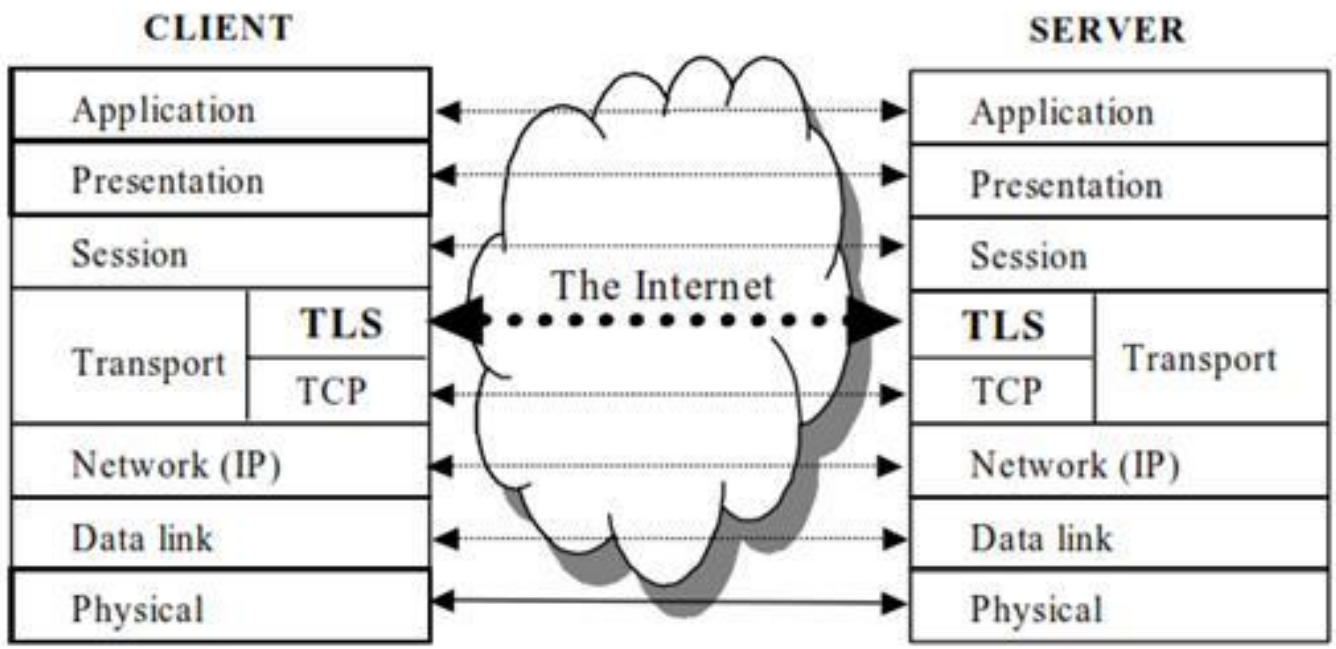
Tipo de certificado	Chave criptográfica			Validade máxima do certificado (anos)
	Tamanho (bits)	Processo de geração	Mídia armazenadora	
A1 e S1	1024	Software	Arquivo	1
A2 e S2	1024	Software	*Smart card* ou *Token*, **sem** capacidade de geração de chave	2
A3 e S3	1024	Hardware	*Smart card* ou *Token*, **com** capacidade de geração de chave	3
A4 e S4	2048	Hardware	*Smart card* ou Token, **com** capacidade de geração de chave	3


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• Protects e-mail messages
• Ensures software came from software publisher
• Protects software from alteration after publication
• Allows data to be signed with the current time
* Refer to the certification authority's statement for details.
Issued to: Autoridade Certificadora Raiz Brasileira
Issued by: Autoridade Certificadora Raiz Brasileira
Valid from 11/30/2001 to 11/30/2011
Install Certificate...
Issuer Statement
Learn more about certificates
OK


Certificate
General
Details
Certification Path
Certification path
Autoridade Certificadora Raiz Brasileira
View Certificate
Certificate status:
This certificate is OK.
Learn more about certification paths
OK

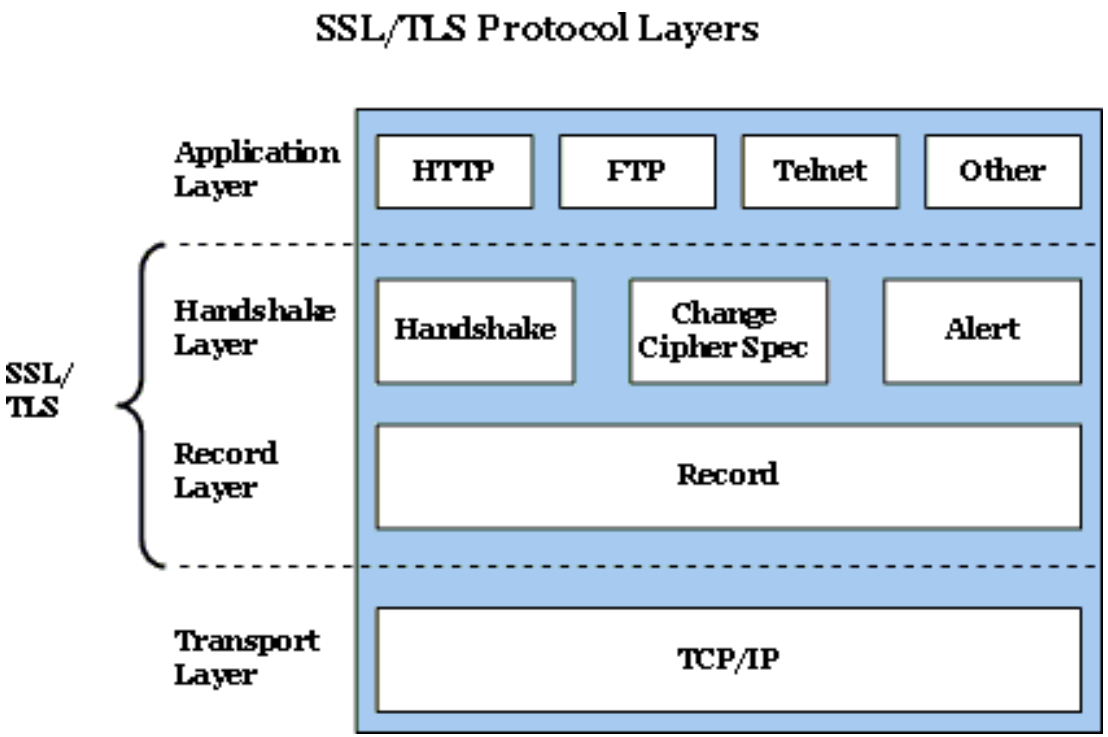
Transport Layer Security (TLS)

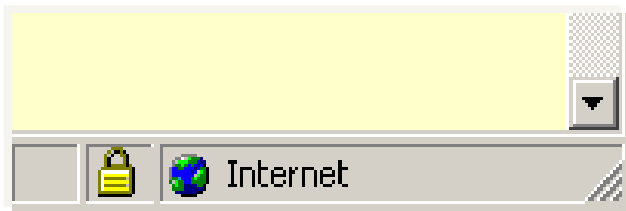
- Protocolo para criptografia e autenticação baseado em sessão
- Fornece um canal seguro entre cliente e servidor
- Funciona na camada de transporte e é independente dos protocolos de aplicativo
- Certificados TLS (SSL) são muito usados na web



TLS

- SSL (Secure Socket Layer) foi originalmente desenvolvido pela Netscape
- Grupo de trabalho TLS (*Transport Layer Security*) foi formado dentro do IETF
- Primeira versão do TLS pode ser vista como SSL v3.1





Símbolo do cadeado denota uso de TLS para segurança Web

Protocolo de Handshake TLS

- **Parte mais complexa do TLS**
- **Permite ao servidor e ao cliente autenticarem um ao outro**
- **Negocia criptografia, algoritmo MAC e chave criptográfica**
- **Usado antes que qualquer dado de aplicação seja transmitido**

Cliente com browser

Loja na Internet com Servidor Web Seguro

1. Cliente conecta com o Lojista

2. Lojista envia cópia do seu certificado (e chave pública) para o browser do cliente, indicando que o SSL está habilitado

3. O browser usa a chave pública da CA para verificar o certificado do lojista

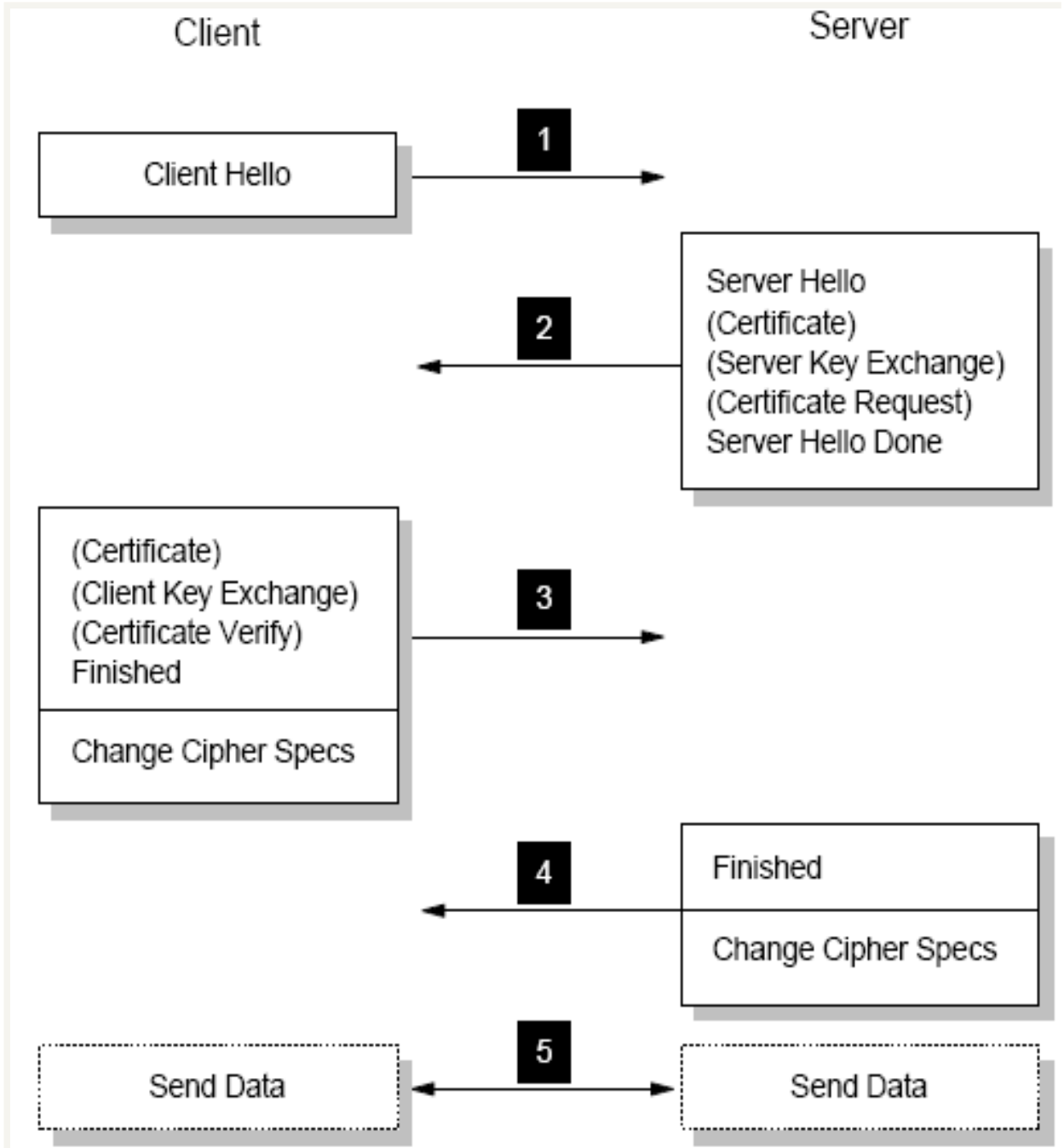
4. O browser gera uma chave de sessão

5. O browser usa a chave pública do Lojista para criptografar a chave de sessão e remete junto o seu certificado

6. O lojista usa a sua chave privada para decodificar a chave de sessão e verifica a assinatura digital do cliente

Cliente e Lojista trocam informações criptografadas com a chave de sessão

Handshake


Client
Server
Client Hello
1
Server Hello
(Certificate)
(Server Key Exchange)
(Certificate Request)
Server Hello Done
2
(Certificate)
(Client Key Exchange)
(Certificate Verify)
Finished
Change Cipher Specs
3
Finished
Change Cipher Specs
4
Send Data
5
Send Data

Mensagens Handshake TLS

- **ClientHello**: lista as capacidades do cliente: versão TLS do cliente, número aleatório de 32 bytes, conjunto de cifras, compressão.
- **ServerHello**: versão TLS do servidor, número aleatório, cifra escolhida, compressão de dados, ID da sessão.
- **Certificate**: servidor envia seu certificado.
- **CertificateRequest**: solicita certificado do cliente (opcional, pouco usado).
- **ServerHelloDone**: indica término do servidor hello
- **ClientKeyExchange**: O cliente gera informações de chave simétrica, codifica-a com a chave pública do servidor e a envia ao servidor.
- **ChangeCipherSpec**: Confirma a chave da sessão e cifra a serem usadas.
- **Finished**: Mensagem de encerramento do handshake. É a primeira mensagem a ser protegida pelos algoritmos e chaves negociados. Após esta mensagem, cliente e servidor podem transmitir dados de maneira segura.