Infra-estrutura de Chaves Públicas

- Esquemas de Autenticação
  - Senhas
    - segredos pessoais
  - Chaves simétricas
    - segredos compartilhados
  - Chaves públicas
    - segredos são distribuídos

Infra-estrutura de Chaves Públicas

- Como distribuir chaves públicas?

INE/UFSC

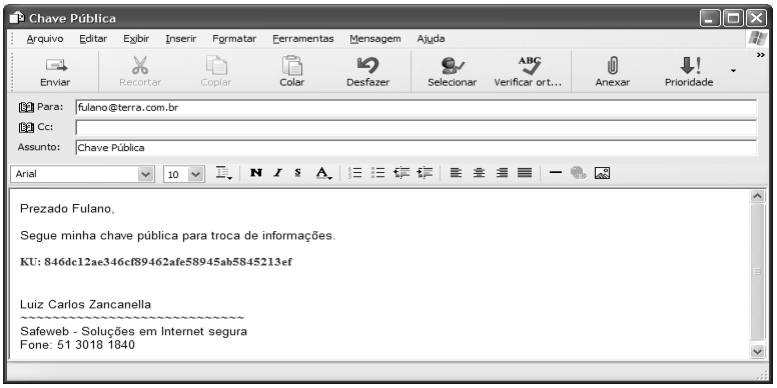
Luiz Carlos Zancanella

e-mail: zancanella@inf.ufsc.br
KU: 846dc12ae346cf89462afe58945ab5845213ef

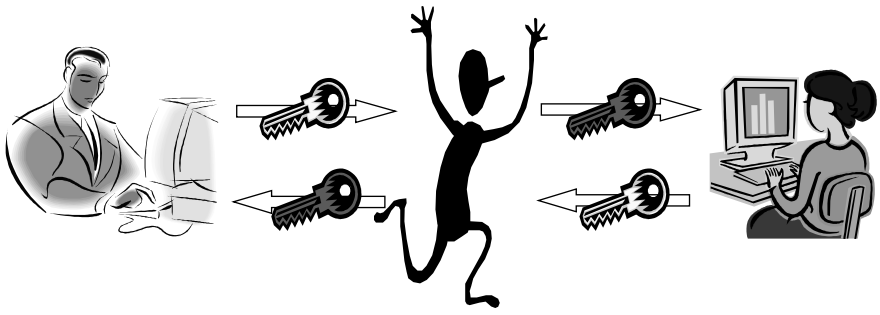
  - Distribuíção da chave pública é pessoal
  - Não há garantia da identidade
  - Como avisar que possuem o cartão, no caso de perda da chave privada correspondente a chave pública

Infra-estrutura de Chaves Públicas

- Como distribuir chaves públicas?

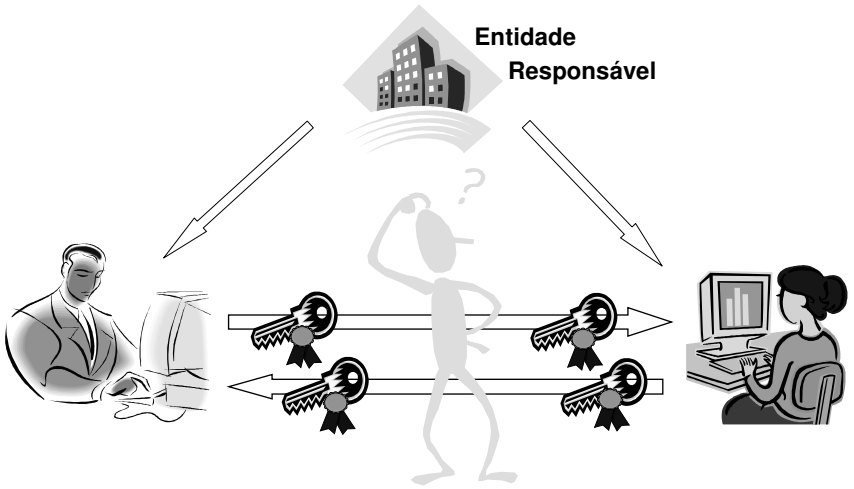


Infra-estrutura de Chaves Públicas



Ataque do homem do meio

Infra-estrutura de Chaves Públicas



Infra-estrutura de Chaves Públicas

- Certificado Ideal
  - Deveria ser puramente digital, podendo ser distribuído pela internet
  - Deveria identificar quem possui a chave privada correspondente ao certificado;
  - Deveria possuir uma entidade responsável pelos dados contidos nele;
  - Deveria ser simples de identificar falsificações;
  - Alterações em seu conteúdo não poderiam ser permitidas;

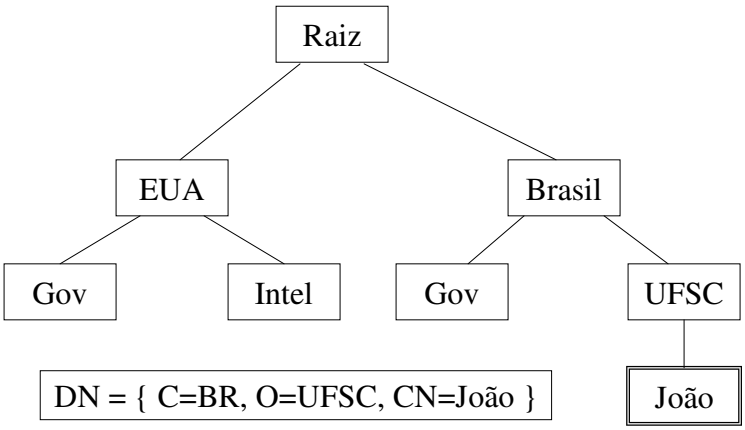
Infra-estrutura de Chaves Públicas

Infra-estrutura
de
Chaves Públicas

Infra-estrutura de Chaves Públicas

Infra-estrutura de Chaves Públicas

Exemplo de um Nome X.500



Infra-estrutura de Chaves Públicas

- **Certificado Digital**

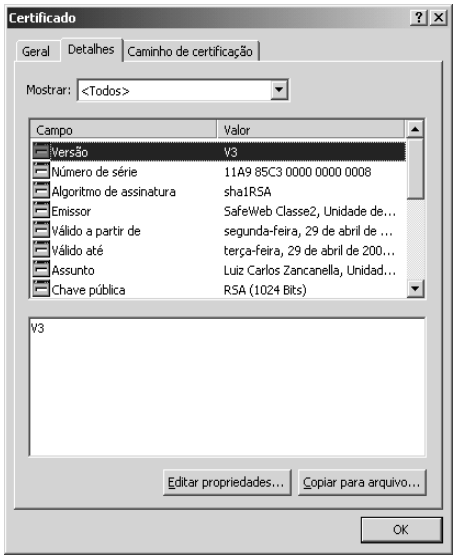
- **Mecanismo utilizado para fazer uma associação entre o nome da entidade (e informações associadas a entidade) com a chave pública correspondente.**

- **X.509** (ITU-T 1997)
- **PGP** (Pretty Good Privacy)
- **SPKI** (Simple Public Key Infrastructure)

Infra-estrutura de Chaves Públicas

- **Versão**

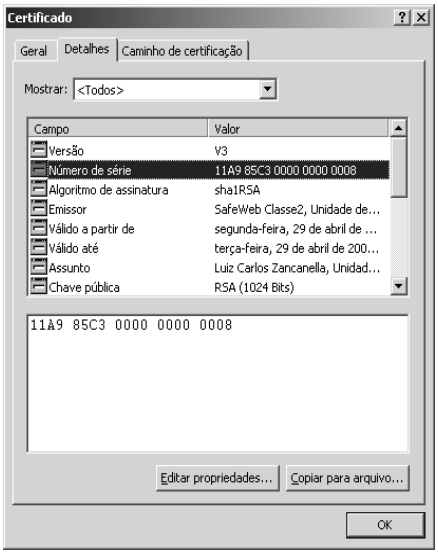
identifica a versão do certificado. O padrão X.509 possue as versões 1, 2 e 3;



Infra-estrutura de Chaves Públicas

- **Número de Série**

Número único que identifica um certificado em relação a Autoridade Certificadora que o emitiu;

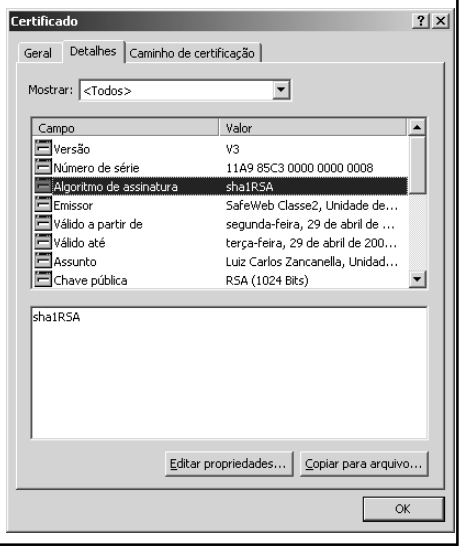


Infra-estrutura de Chaves Públicas

- **Algoritmo de assinatura**

Identifica o algoritmo usado pela Autoridade Certificadora para criar o resumo e assinar o certificado.

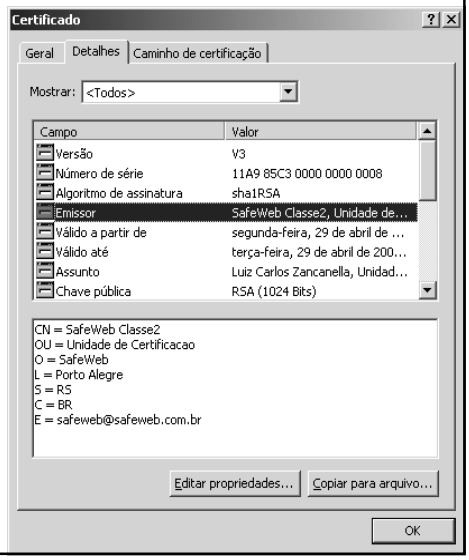
ex:
SHA1 – algoritmo de hash
RSA – algoritmo de criptografia



Infra-estrutura de Chaves Públicas

- **Emissor**

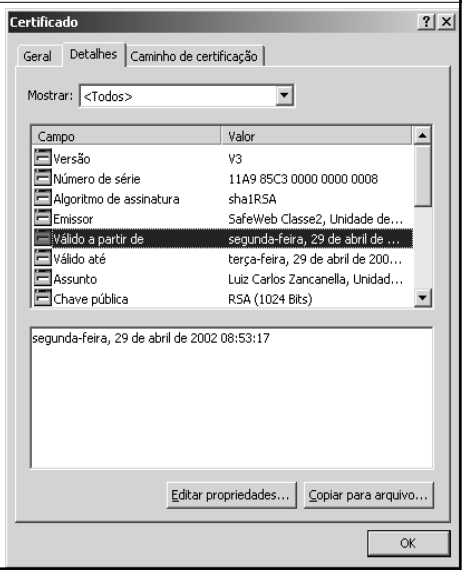
Informações que identificam a Autoridade Certificadora que emitiu o certificado;



Infra-estrutura de Chaves Públicas

- **Período de validade**

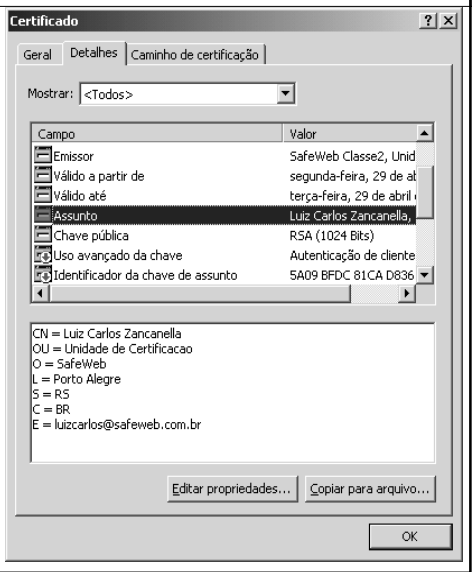
Intervalo de tempo que um certificado pode ser considerado válido. Este campo possui a data que o certificado foi emitido pela Autoridade Certificadora e sua data de expiração;



Infra-estrutura de Chaves Públicas

- **Assunto (entidade)**

Dados de identificação da entidade para a qual o certificado foi emitido



Infra-estrutura de Chaves Públicas

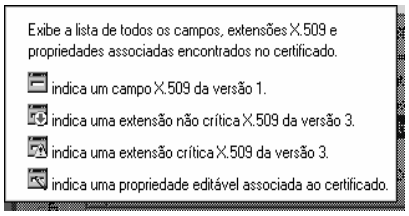
- **Chave pública**

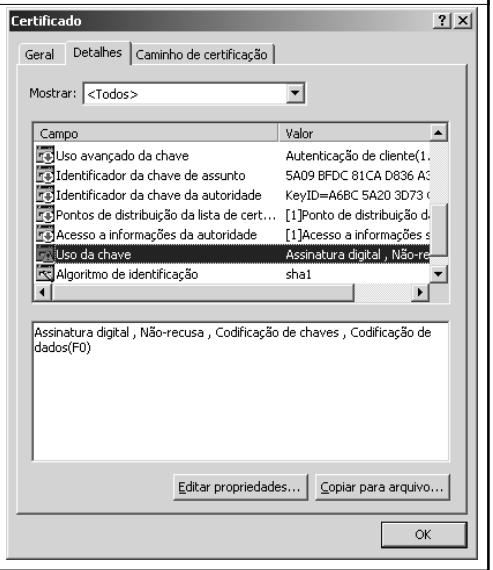
Chave pública (e identificação do algoritmo) associada a entidade do certificado.

Infra-estrutura de Chaves Públicas

- **Uso da Chave**

Indica o(s) propósito(s) para o qual a chave pública do certificado pode ser utilizada.





Infra-estrutura de Chaves Públicas

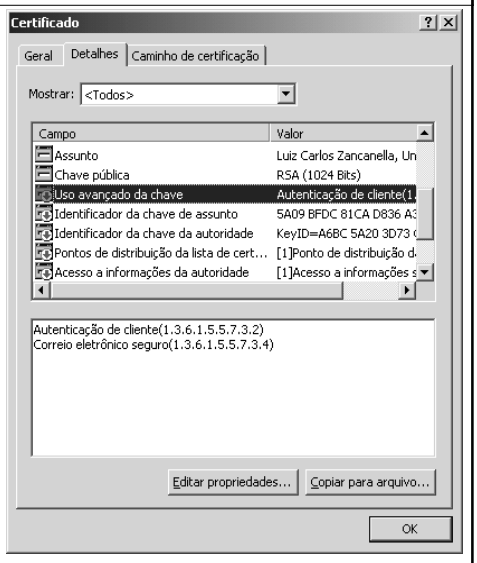
- **Uso extendido da Chave**

Indica o propósito para o qual a chave pública do certificado pode ser utilizada, em adição ou substituição ao propósito definidos no campo "Uso da Chave".

The following OIDs matched

- 1.3.6.1.5.5.7.3.1 - id_kp_serverAuth
- 1.3.6.1.5.5.7.3.2 - id_kp_clientAuth
- 1.3.6.1.5.5.7.3.3 - id_kp_codeSigning
- 1.3.6.1.5.5.7.3.4 - id_kp_emailProtection
- 1.3.6.1.5.5.7.3.5 - id-kp-ipsecEndSystem
- 1.3.6.1.5.5.7.3.6 - id-kp-ipsecTunnel
- 1.3.6.1.5.5.7.3.7 - id-kp-ipsecUser
- 1.3.6.1.5.5.7.3.8 - id_kp_timeStamping

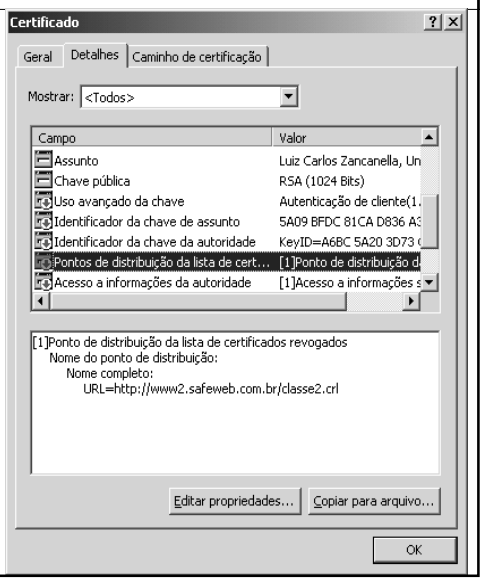
IANA – Internet Assigned Number Authority



Infra-estrutura de Chaves Públicas

- **Pondo de distribuição da LCR**

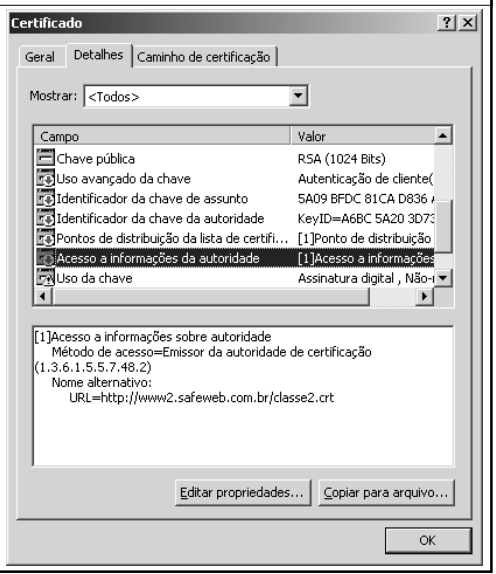
Indica o local, ou locais, onde a LCR correspondente ao certificado está armazenada. A aplicação cliente encontrará a LCR atualizada, para conferir se o certificado em processamento está revogado.



Infra-estrutura de Chaves Públicas

- Informações da autoridade

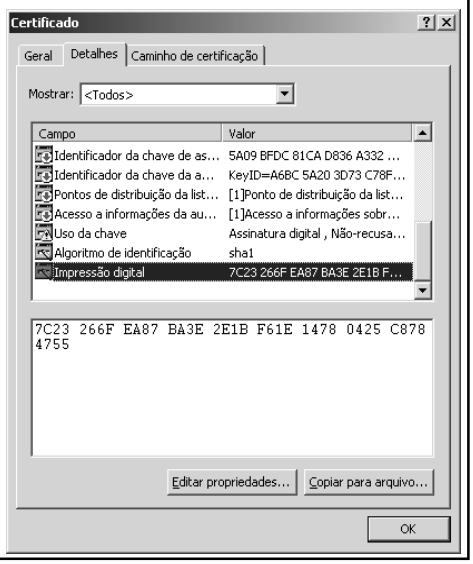
Extensão utilizada para acessar o certificado da autoridade de certificação que assinou o certificado.



Infra-estrutura de Chaves Públicas

- **Impressão digital**

Contém o hash do certificado digital, efetuada pela autoridade certificadora imediantamente acima na hierarquia do caminho de certificação, para garantir a identificação do certificado.



Infra-estrutura de Chaves Públicas

- **Extensões**

  Somente disponível na versão 3 da recomendação X.509, os campos de extensões tem a finalidade de tornar mais flexível a utilização dos certificados digitais.

  dois grupos: críticas e não-críticas. Uma aplicação pode ignorar uma extensão não-crítica, caso ele não a reconheça. Porém, a aplicação deve rejeitar um certificado que possua uma extensão crítica que não seja reconhecida.

Infra-estrutura de Chaves Públicas

Extensões Particulares

Uma AC, ou uma empresa, pode inserir extensões cuja finalidade somente elas conhecem. A criação deste tipo de extensão facilita o desenvolvimento de aplicativos personalizados. Além disso, possibilita a inserção de dados que não podem ser adequados aos campos e extensões definidos pela recomendação.

Um exemplo de uso de extensões particulares é a definição de níveis de acesso a um determinado sistema. Pode ser inserida uma ou várias extensões contendo os privilégios de determinados usuários para aquele sistema. Desse modo é possível validar um usuário através de valores contidos em seu certificado.

Infra-estrutura de Chaves Públicas

- **Extensões Particulares**

  OID, Bit de criticalidade, Valor

  UFSC OID : 1.3.6.1.4.1.7687

  Valor : tipo de dado, valor

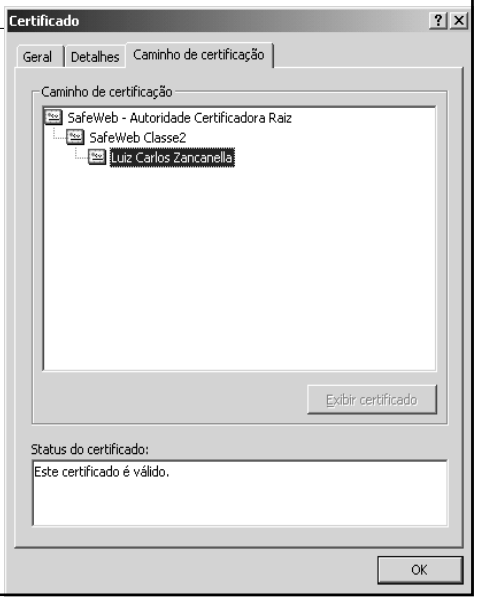
  Ex: **1.3.6.1.4.1.7687.1 – LabSec**
  1.3.6.1.4.1.7687.1.1 – Nível de acesso ao sistema

  1.3.6.1.4.1.7687.1.1, 0, 1 – acesso a professores
  1.3.6.1.4.1.7687.1.1, 0, 2 – acesso a alunos

Infra-estrutura de Chaves Públicas

- **Caminho de certificação**

  Consiste em uma cadeia de certificados relacionados.



Infra-estrutura de Chaves Públicas

- **Status do certificado**

  Indica se o certificados é um certificao válido, ou o motivo pelo qual o certificado está inválidado.

Infra-estrutura de Chaves Públicas

Certificado Servidor

autenticação servidor

- Assegura a identidade do site;
- Garante a integridade dos dados;
- Troca de dados de modo sigiloso;

Infra-estrutura de Chaves Públicas

Certificado Pessoal

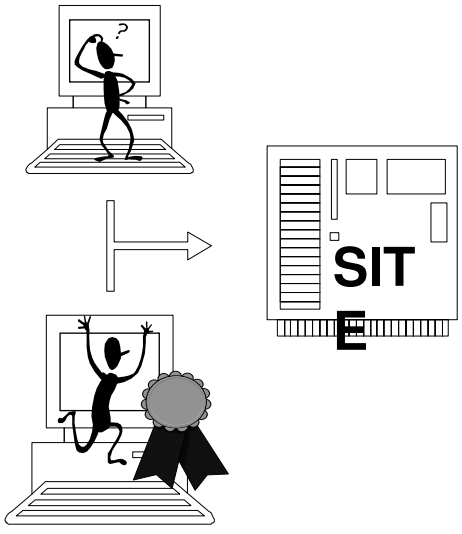
uso em documentos eletrônicos

- **Assinatura**
  - **Autenticidade,**
  - **Integrigade,**
  - **Não-repúdio.**
- **Criptografia**
  - **Sigilo**

Infra-estrutura de Chaves Públicas

Certificado Pessoal

uso na identificação de acesso



Infra-estrutura de Chaves Públicas

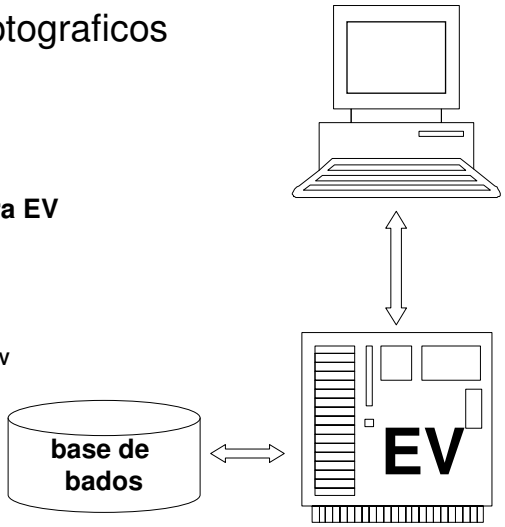
Uso em Protocolos Criptograficos

Votante,

- **assina o voto com KR_v**
- **cifra o voto com KU_{EV}**
- **envia voto + assinatura para EV**

Entidade de Votação,

- **descifra o voto com KR_{EV}**
- **verifica assinatura com KU_V**



Infra-estrutura de Chaves Públicas

Diretório Público

- Local na Internet/Intranet onde ficam disponíveis informações de acesso público. Ex: Certificados Digitais, Listas de Certificados Revogados, etc..

- O diretório não necessita estabelecer uma conexão segura. Porém ele deve garantir a integridade e atualidade das informações disponíveis.

Infra-estrutura de Chaves Públicas

Módulo Público

- Interface disponível para o usuário interagir com os demais componentes da Infra-estrutura de Chaves Públicas;
- O usuário não pode ter acesso a determinados componentes, então usa o módulo público para efetuar as tarefas;

Infra-estrutura de Chaves Públicas

Entidade de Registro

- Responsável pela verificação das informações contidas na solicitação de um certificado digital;
- Uma Autoridade Certificadora pode possuir várias Autoridades de Registro vinculadas;

Infra-estrutura de Chaves Públicas

- **Listas de Certificados Revogados (CRL)**

Objetivo:

Manter uma relação dos certificados que não devem mais ser considerados válidos.

Um certificado somente pode ser revogado durante sua data de validade;

Segue a recomendação X.509 do ITU-T

Infra-estrutura de Chaves Públicas

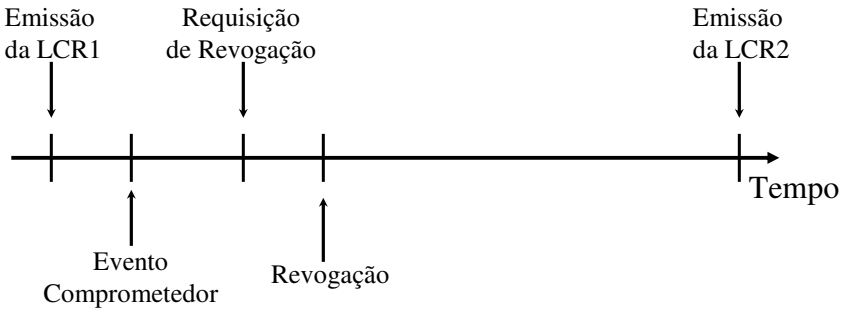
- **Listas de Certificados Revogados (CRL)**

Possíveis motivos para revogação de um certificado

- Comprometimento da chave da privada do certificado;
- Comprometimento da chave da privada da autoridade certificadora;
- Mudança de filiação;
- Atualização cadastral;
- Cancelamento da operação;
- Suspensão temporária;
- Não específico;

Infra-estrutura de Chaves Públicas

- **Listas de Certificados Revogados (CRL)**



Infra-estrutura de Chaves Públicas

- **Modelos de Confiança**

Modelo Isolado

- Possui uma única Autoridade Certificadora Raiz (AC-Raiz);
- A AC Raiz pode assinar várias Autoridades Certificadoras;
- Podem existir vários níveis de Autoridades Certificadoras abaixo da AC-Raiz;