PKI

Felipe Fonseca
Lucas Tostes
Thaiana Lima

Agenda

1. Introdução
2. Modelos de confiança
3. Certificados
4. Controle de acesso
5. Conclusão

Introdução

Introdução

- Criptografia assimétrica é muito utilizada
- Garante segurança na comunicação
- Como garantir autenticidade da chave?

Introdução

- Emissão de certificados por Autoridades Certificadoras (CA)

- Maior garantia de que a pessoa é quem diz ser

Modelos de confiança

Modelos de confiança

- Monopólio
- Uma única CA para todos
- Pode usar Autoridades Registradoras (AR)

Modelos de confiança

- Oligarquia
- Utilizada nos navegadores
- Lista de CA's cadastradas

Modelos de confiança

- Anarquia
- Não existem CA's
- Cada usuário é responsável por manter sua lista de confiança

Modelos de confiança

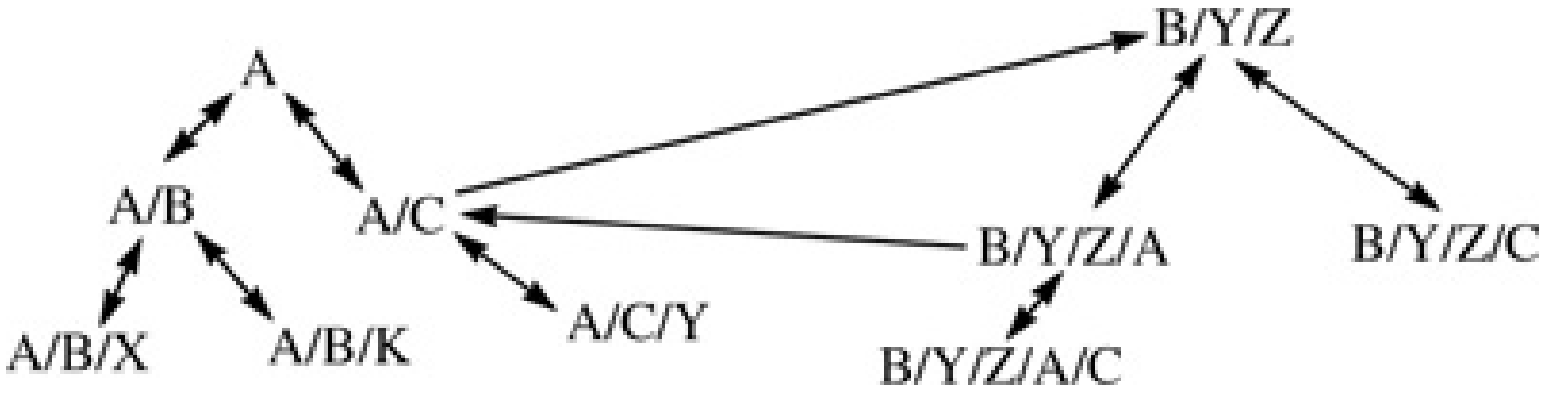
- Restrição de nomes
- CA's possuem confiança limitada
- Hierarquia de nomes

Modelos de confiança

- Restrição de nomes Bottom-up
- Modelo teórico
- Redes hierárquicas com ligações entre si

Modelos de confiança

- Restrição de nomes Bottom-up



Certificados

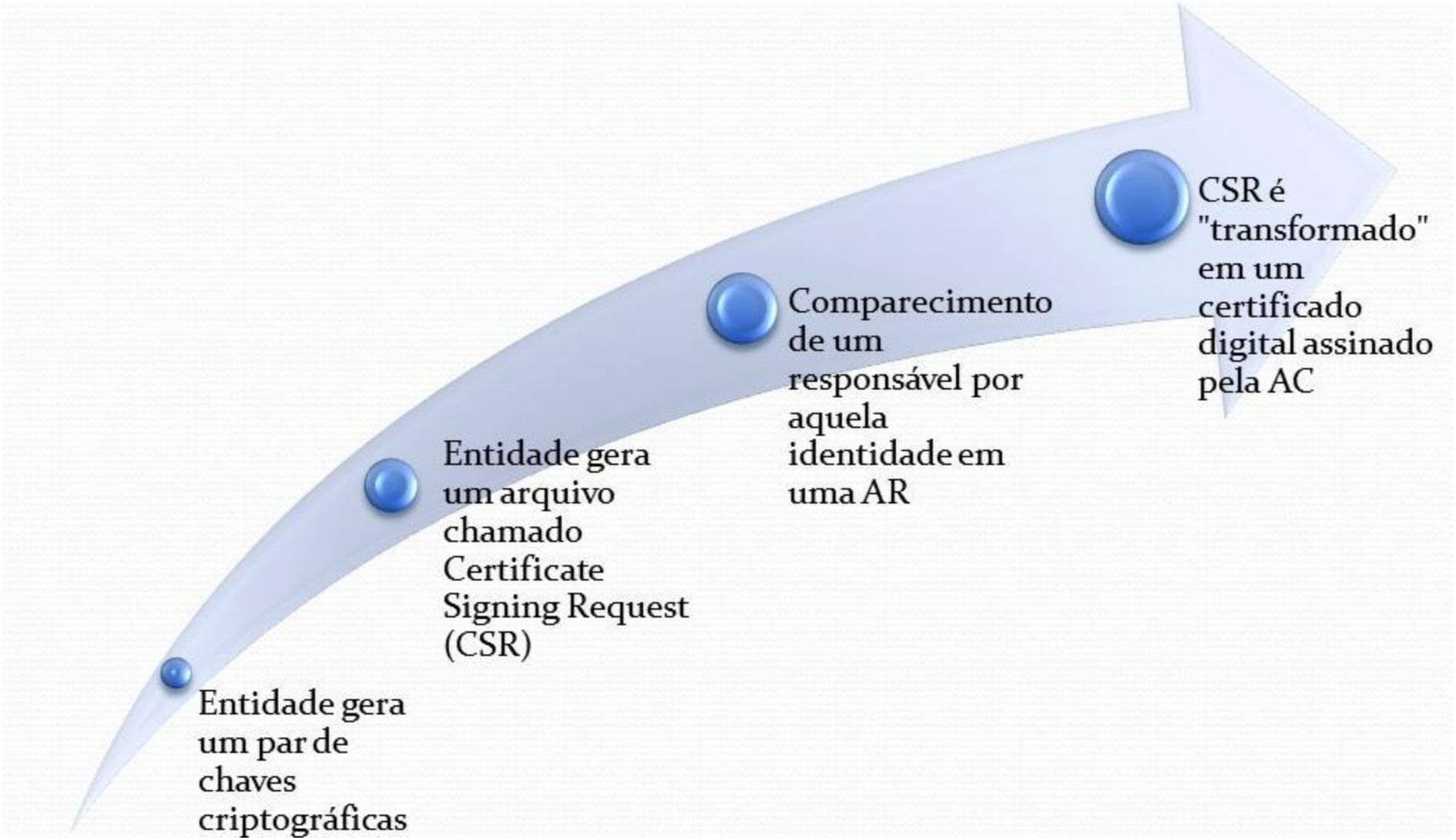
Certificados

- Comprova a identidade de um usuário.
- Certificação com assinatura digital, emitido por uma instituição de confiança (CA).
- É assinado utilizando própria chave privada do certificador.

Certificados – padrão X.509

- Certificado contém diversas informações, além da chave pública.
- Padrão X.509, atualmente possui 3 versões.
- Informações como:
  - Número serial
  - Nome do CA emissor
  - Chave pública do usuário a ser certificado
  - Validade

Criando um certificado



Certificados - Revogação

- Certificate Revocation Lists (CRLs)

- Repositórios de CRLs

- Processo:
  - A entidade pede ao RA para ter seu certificado revogado;
  - RA decide e possivelmente passa para o CA
  - CA atualiza a CRL e publica no repositório;

Empresas certificadoras

Controle de Acesso

Controle de Acesso

- Controla os privilégios de um usuário.
- Exige a autenticação para acesso (certificado)

Controle de Acesso

- PKI

- Comunicação ***vs*** Busca e recuperação de dados

Controle de Acesso

- ACL - *(Lista de Controle de Acesso)*
- Centralização
- Escalabilidade?

Controle de Acesso

- Divisão em Grupos
- *Roles* - (Papéis)
- Sistemas Intra-Organizacionais
- Grupos Invisíveis

Conclusão

Conclusão

- Aumenta a confiança na rede
- Emite certificados com validade
- Possui diversos modelos de implementação
- Não garante segurança total

Perguntas

Perguntas

1 - O que é PKI e qual a sua importância?

Perguntas

1 - O que é PKI e qual a sua importância?

R: Infraestrutura de chave pública. Ela é importante para verificar a identidade de um usuário com mais confiança.

Perguntas

2 - Descreva o modelo de confiança Anarquia e cite uma vantagem e uma desvantagem.

Perguntas

2 - Descreva o modelo de confiança Anarquia e cite uma vantagem e uma desvantagem.

R: No modelo anarquia cada usuário é responsável por definir suas âncoras de confiança. Uma vantagem que não há tarifas para obter um certificado e uma desvantagem é que a rede fica sujeita mais facilmente a inclusão de falsos certificados

Perguntas

3 - Cite 2 maneiras de saber se um certificado é válido.

Perguntas

3 - Cite 2 maneiras de saber se um certificado é válido.

R: a- Verificando a CRL, pode não ser um método muito confiável porque vários certificados são revogados por dia. Se uma empresa possui uma CRL desatualizada, pode estar confiando em um certificado que foi recentemente revogado.

b- verificando a data de validade do certificado

Perguntas

4 - Porque é incomum o Controle de Acesso em PKI?

Perguntas

4 - Porque é incomum o Controle de Acesso em PKI?

R: a- Pois o foco de ambientes PKI é na segurança na comunicação e não na busca e recuperação de dados.

b- O investimento em PKI é focado em larga escala, onde o suporte a Controle de Acesso é complexo.

Perguntas

5 - Como a PKI evita que pessoas mal intencionadas se passem por outras?

Perguntas

5 - Como a PKI evita que pessoas mal intencionadas se passem por outras?

R: Através dos certificados e das chaves públicas registradas, as autoridades certificadores podem comprovar a veracidade da informação que está sendo enviada.

Referências

1. Certificate-Based Authorization Policy in a PKI Environment - MARY R. THOMPSON, ABDELILAH ESSIARI, and SRILEKHA MUDUMBAI
2. Developing a Public Key Infrastructure for Use in a Teaching Laboratory - Phillip T. Rawles and Kristoffer A. Baker
3. PKI (*Public Key Infrastructure*): Abordagens Utilizando Sistemas *Opensource* - Marcelo Santos Daibert
4. Network Security: Private Communication in a Public World, Second Edition – Charlie Kaufman, Radia Perlman and Mike Speciner
5. PKI and Access Control in Office Environments – Christopher Woodward and Wasim A Al-Hamdani
6. Public Key Infrastructure visualization – Derek Ebeling and Rob Santos
7. Simple Certified e-Check with a Partial PKI solution – Wen-Jung Hsin and Lein Harn
8. Gestão de Segurança da Informação – Marcos Aurelio Pchek Laureano
9. http://pt.scribd.com/doc/52039074/40/PKI-Public-Key-Infrastructure (Último acesso: 24/05/2012)