Apontamentos Slides04

- **Geração de chaves**
  - **Princípios:**
    - **Utilizar geradores bons na produção de segredos**
    - Resultados é indistinguível de ruído
    - Não existem padrões derivados no número da iteração ou valores anteriores
    - **Facilitar os processos sem comprometer a segurança**
    - **Chaves públicas eficientes:**
      - Dimensão reduzida
      - Acelera operações com chaves públicas
      - Não adiciona questões de segurança
    - **A chave privada deve ser gerada pelo próprio**
      - Para assegurar ao máximo a sua privacidade
        - Melhor: O dono também não ter a chave, apenas acesso aos processos com ela
      - Este princípio pode ser relaxado se não se pretender assinaturas digitais
  - **Cuidados:**
    - Correção:
      - A chave privada representa um sujeito pelo qie o risoc do seu comprometimento deve ser minimizado
        - Cópias de salvaguarda
      - O caminho de acesso à chave deve ser controlado
    - Confinamento
      - Armazenamento da chave numa entidade autónoma segura
      - Utilização protegida da chave

- **Distribuição de chaves públicas**
  - **Enviar** informação **confidencial:**
    - Manual
    - Protegida por um segredo confidencial
    - Certificados digitais
  - **Validar** informação **autenticada:**
    - Manual
    - Certificados digitais
  - Disseminação confiável de chaves públicas
    - Se A confia em K e B confia em A então B confia em K
  - Hierarquias e grafos de certificação

- **Certificados digitais de chaves públicas**
- **Documentos digitais emitidos por uma Entidade Certificadora (EC)/Certification Authority (CA)**
    - Ligam uma chave pública a uma entidade
    - São documentos públicos
    - São seguros por meio criptográficos
        - Fingerprint
        - Assinatura digital criada pelo emissor (CA)
- **Usados para distribuir chaves públicas de forma confiável**
    - Os verificadores podem validar os documentos
    - Os verificadores confiam no comportamento das CA

- **Utilização de um par de chaves**
    - O certificado associa um par de chaves a um perfil de **utilização restrito**
        - Uma entidade terá vários certificados, um para cada utilização (Key Usage)
    - Perfis típicos
        - Autenticação / Distribuição de chaves
            - Assinaturas digitais, cifra de chaves, cifra de dados, negociação de chaves
        - Assinatura de documentos
            - Assinaturas digitais
        - Emissão de certificados
            - Assinaturas de certificados e objetos relacionados

---

- **Entidade Certificadoras (CA)**
    - **Organizações que gerem certificados de chave pública**
        - Importante que operem corretamente para serem confiáveis
        - Gerem também processos de revogação de certificados
    - **CA confiáveis**
        - Entidades certificadoras raiz
        - Entidades certificadoras intermédias: Certificadas por outra CA
        - Raízes de confiança ou raízes de certificação
            - Alguém possui e confia numa chave pública
            - Certificados das CAs são auto assinadas
                - Podem também ser assinados por outras Cas
            - Distribuição manual

- PEM
    - Nunca implementado globalmente
    - Hierarquias independentes sem uma raiz única

    - Cada CA raiz negocia a distribuição da sua chave pública em cada entidade
- PGP
    - Segue um modelo baseado numa rede de confiança
    - Sem qualquer autoridade central de confiança
    - Pessoas usam dois tipos de confiança
        - Confiança nas chaves que conhecem
        - Confiança no comportamento de outros certificadores

---

- **Refrescamento de chaves assimétricas**
    - Pares de chaves devem ter uma validade limitada
    - **Problemas**
        - Os certificados podem ser copiados e distribuídos livremente
        - O universo de possuidores de certificados é desconhecido
    - **Soluções**
        - Certificados com uma validade temporal definida
        - Lista de Revogação de certificados (CRL)
            - Para permitir revogar certificados antes que expirem

---

- **Listas de Revogação de certificados (CRL)**
    - Listas assinadas com identificadores de certificados revogados prematuramente
        - Devem ser consultados periodicamente pelos verificadores
        - Entradas podem conter a razão
    - Publicação e distribuição de CRLs
        - Cada CA possui a sua CRL, de acesso público
        - CAs trocam CRLs para facilitar distribuição
    - Vários formatos disponíveis
        - Base CRL
        - Delta CRL
        - OCSP
- **OCSP**
    - Protocolo baseado em HTTP para verificar a revogação de certificados
    - Reduz a largura de banda usada por clientes
    - Pode envolver maior largura de banda das CAs
    - **OCSP Stapling**
        - Inclui um instante temporal assinado na resposta
        - Clientes podem guardar respostas durante a sua validade

---

- **PKI: Public Key Infrastructure**
    - Infraestrutura de apoio ao uso de pares de chaves e certificados
    - Criação segura de pares de chaves assimétricas
    - Criação e distribuição de certificados de chaves públicas

- Definição e uso de cadeias de certificação
- Atualização, publicação e consulta de listas de certificados revogados
- Uso de estruturas de dados e protocolos que permitem a interoperação entre componentes

- **Relações de confiança**
  - Um PkI estabelece relações de confiança de duas formas
    - Emitindo certificados de chaves públicas de outras CAs
    - Requerendo a certificação da sua chave pública a outras CAs
  - Relações de confiança características
    - Hierárquicas
    - Cruzadas
    - Ad-hoc
- **Fixação dos Certificados (Pinning)**
  - Se um atacante possui acesso a uma raiz de confiança, ele pode emitir qualquer certificado para qualquer entidade
    - Manipular a CA para que ela emita um certificado
    - Injetar raízes adicionais nos sistemas da vítima
  - Certificate Pinning: Adicionar uma impressão digital da chave pública ao código
  - Processo de validação normal + verificação de impressão digital
    - Certificado tem de ser assinado por uma reaiz de confiança
    - Certificado tem de ter uma chave pública com a impressão digital especificada

---

- **Transparência de Certificação**
  - Problemas:
    - CAs podem ser comprometidas
    - Comprometimento é difícil de detetar
  - Definição: **Sistema que regista todos os certificados públicos emitidos**
    - Garante que só são publicados certificados que levam a raízes legítimas
    - Armazena toda a cadeia de certificação de cada certificado
    - Apresenta esta informação para auditoria
      - Organizações ou ad-hoc pelos utilizadores