Conteúdo para a frequência de Criptografia Aplicada 2

Assinaturas digitais

As assinaturas digitais permitem, **autenticar conteúdos de um documento** (integridade), **autenticar a origem do documento** (autenticidade) e garantir a **não repúdio** (não negação da autoria).

As assinaturas digitais são compostas por **dois algoritmos**:

- **Geração de assinaturas**: produção de um valor usando a **chave privada**;
- **Verificação de assinaturas**: validação do valor usando a **chave pública**.

Existem dois **esquemas de assinatura digital**:

- **Esquema de assinatura com apêndice**: a assinatura é separada do mensagem. A mensagem pode ser visualizada sem a assinatura validada;
- **Esquema de assinatura com recuperação de mensagem**: a assinatura é incluída na mensagem. A mensagem não pode ser visualizada sem a assinatura validada.

Algoritmo de geração de assinaturas

Para **esquemas de assinatura com recuperação de mensagem**:

- É assinado o documento, Assinatura(Mensagem) = informação + E(Priv, documento)
- Para verificar a assinatura, extraimos a chave pública das informações e, D(Pub, Assinatura) e verificamos a integridade do documento.

Para **esquemas de assinatura com apêndice**:

- É assinado o documento, Assinatura(Mensagem) = E(Priv, Hash(Mensagem))
- Para verificar a assinatura, extraimos a chave pública das informações e, D(Pub, Assinatura) = hash'(Mensagem) e verificamos se o hash' é igual ao hash da mensagem.

Elementos principais de uma assinatura digital:

- A mensagem a assinar;
- Data da assinatura;
- Identificação do assinante;

A **data da assinatura** pode ser:

- Dada pela máquina que assina;
- Dada por uma **entidade de confiança** (TSA ou Time Stamp Authority).

TSA (Time Stamp Authority)

A **Time Stamp Authority** é uma entidade de confiança que fornece **carimbos de tempo**.

Estes carimbos de tempo são usados para **provar a existência de uma mensagem** num determinado momento e proteje contra **ataques de falsificação**.

É feito o hash da mensagem, o mesmo é contatenado com a data e é assinado o hash dessa contatenação com a chave privada da TSA.

A **identificação do assinante** pode ser:

- Fornecida por um **certificado de chave pública**;

Certificado de chave pública

Este certificado fornece:

- Diversos atributos de identificação do assinante;
- A chave pública do assinante, para verificação da assinatura;
- Prazo de validade do certificado;
- **CRL** (Certificate Revocation List) ou **OCSP** (Online Certificate Status Protocol) para verificar a validade do certificado.

A assinatura digital pode também ter **elementos opcionais**:

- **Localização de onde foi assinado**;
- **Motivo da assinatura**;
- etc.

Assinaturas digitais com RSA

- Criação de assinaturas com a chave privada, validação com a chave pública;
- Padding especial para esquemas de assinatura com apêndice (i.e. RSASSA-PSS e RSASSA-PKCS1-v1_5);
- Prefixação com o algoritmo de hash usado (i.e. ASN.1);

ASN.1 prefixação

É composto por um **OID** (Object Identifier) que contém o algoritmo de hash usado. Este OID é seguido pelo **hash** da mensagem.

Standards de assinatura digital (DSS)

Existem dois standards de assinatura digital:

- Com a variante do **ElGamal** (DSA);
- Com curvas elípticas (ECDSA);

Blind signatures

É um esquema de assinatura digital que permite que uma entidade assine uma mensagem sem saber o conteúdo da mesma. É usado para garantir a anonimidade de uma mensagem.

Implementação, usando RSA:

Escolha do Fator do Blinding Factor - k: Gere um número aleatório K.

Propriedade do Fator de Ofuscação: Garanta que K × K^(-1) ≡ 1 (mod N), onde N é o módulo da chave RSA.

Ofuscação da Mensagem (m'): Calcule m' = K^e × m mod N, onde e é a chave pública de RSA.

Assinatura Usando a Chave Privada (Ax(m')): Compute Ax(m') = (m')^d mod N, onde d é a chave privada de RSA.

Unblinding da Assinatura (Ax(m)): Calcule Ax(m) = K^(-1) × Ax(m') mod N.

Assinatura eletrónica qualificada

Para uma assinatura eletrónica ser qualificada, é necessário:

- Ser compatível com a regulamentação da UE eIDAS;
- Permite a verificação de autoria por longos períodos de tempo;
- Pode ser considerado o equivalente eletrónico de uma assinatura manuscrita;

Contém **três requisitos**:

- A pessoa que assina deve ser vinculada e identificada de forma inequívoca à assinatura;
- Os dados usados para criar uma assinatura devem estar sob o controle exclusivo do signatário;
- Deve ser possível detectar alterações nos dados assinados;

Estas assinaturas pode ser produzidas por **dispositivos criptográficos qualificados**, como:

- Cartão do cidadão;
- Smart card;
- Chave Móvel Digital;

Estes dispositivos dão uma nova camada de segurança, pois:

- A chave privada não sai do dispositivo (não pode ser copiada nem exportada);
- Além da portação física, é necessário um segundo fator de autenticação (PIN);
- São certificadas por uma entidade de confiança;

PKCS #11

É uma API que permite a utilização de dispositivos criptográficos (i.e. cartão do cidadão) e que permite a utilização de chaves privadas e a realização de operações criptográficas.

Long-Term Validation (LTV)

Este mecanismo foi criado devido à possível obsolescência de algoritmos criptográficos ao longo do tempo e à possível invalidez do par de chaves devido a prazo de validade expirado.

É um mecanismo que permite a validação de assinaturas digitais de um modo intemporal, mesmo que o algoritmo de assinatura tenha ficado inválido ou o certificado esteja revogado. Isto é feito através de **camadas de assinatura**.

Proof of Existence

É um mecanismo que permite provar que um determinado documento existia numa determinada data.

Caso um documento possa ser validado agora e o timestamp esteja vinculado a valores que eram válidos quando foi assinado, então esses valores são válidos agora.

Tipos de assinaturas:

- PAdES (PDF Advanced Electronic Signatures);
- CAdES (CMS Advanced Electronic Signatures);
- XAdES (XML Advanced Electronic Signatures);

Gestão de chaves assimétricas

A gestão de chaves assimétricas **permite**:

- Saber quando e como as chaves foram geradas;
- Como as chaves privadas são protegidas;
- Como as chaves públicas são distribuídas;
- Prazo de validade do par de chaves;

A geração de chaves assimétricas **deve ser feita**:

- **Usando bons PRNGs** (Pseudo Random Number Generator);
- **Facilitar a geração sem comprometer a segurança**;
- **Auto geração da chave privada**;

Exploração da chave privada

A chave privada deve:

- Ter a sua comprometidão minimizada;
- Confinada (isolada) a um dispositivo seguro;

Distribuição do certificado de chave pública

A chave pública deve ser distribuída entre:

- **Remetentes** de dados confidenciais;
- **Recepetores** de dados assinados;

Esta distribuição pode ser feita por:

- **Cadeia de certificados**;
- **Transitivade de confiança** (se A confia em B e B confia em C, então A confia em C);

Pode ser feita através de:

- **Modo explícito**: pedido de modo voluntário pelo utilizador;
- **Modo implícito**: pedido do utilizador a um serviço para obter um certificado necessário (i.e. acesso a um website).

Os certificados de chave pública são emitidos por **entidades de confiança** (CA ou Certificate Authority).

Utilização do par de chaves

Um par de chaves está ligado a um perfil de utilização pelo certificado de chave pública.

Utilizações:

- **Autenticação**;

- **Assinatura de documentos**;
- **Emissão de certificados**;

Para classificar a sua utilização, existem **extensões**, identificadas por um **OID**:

- Uma **extensão crítica**: se não for reconhecida, o certificado não é válido;
- Uma **extensão não crítica**: mesmo se não for reconhecida, o certificado é válido;

Cadeia de certificados

A cadeia de certificados é uma **lista de certificados** que permite validar um certificado de chave pública.

É composta por:

- **Certificado de chave pública**;
- **Certificado de chave pública da(s) CA(s)**;
- **Certificado de chave pública do CA raiz (root)**;

Autoridade de certificação (CA)

É uma entidade de confiança que emite certificados de chave pública.

Define **politicas de certificação**:

- Emissão de certificados;
- Revogação de certificados;
- Distribuição de certificados;
- Emissão e distribuição da chave privada correspondente;

Tipos de CA:

- **CA raiz (root)**: emite certificados de chave pública para outras CA;
- **CA intermédia**: emite certificados de chave pública para utilizadores finais;

Existem **modelos de hierarquia de certificados**:

- **PGP**: rede de confiança, onde não existe uma autoridade central e cada utilizador é uma CA. Existem dois tipos de confiança:
  - **Marginal**: o utilizador confia no certificado, mas não confia na capacidade do utilizador de verificar outros certificados;
  - **Completamente**: o utilizador confia no certificado e na capacidade do utilizador de verificar outros certificados;
- **PEM**: hierarquia de certificados, onde existe uma CA raiz e CA intermédias (nunca implementado: floresta de hierarquias, onde cada CA raiz negoceia a distribuição de chaves públicas com outras CA raiz);

Atualização de chaves assimétricas

Estes pares de chaves devem ter um **prazo de validade**, pois a sua segurança pode ser comprometida.

Os certificados de chave pública podem ser distribuidos livremente, por isso existe:

- Certificados com **prazo de validade**;
- Lista de certificados **revogados** (CRL ou Certificate Revocation List);

CRL (Certificate Revocation List)

É uma lista de certificados revogados, emitida por uma CA. Pode ser do tipo:

- Base: lista de certificados revogados;
- delta: lista de certificados revogados desde a última lista base;

Validações de Certificados Individuais:

- **OCSP (Online Certificate Status Protocol)**: protocolo que permite verificar o estado de um certificado;
- OCSP Stapling: permite que o servidor web verifique o estado do certificado;

Distruibuição de CRLs é feita por:

- Cada CA publica a sua CRL;
- As CAs trocam entre si as suas CRLs;

Ao ser revogada:

- A chave privada pode ser usada para assinar, porém é inválida;
- A chave pública pode ser usada a qualquer momento;

Infraestrutura de chaves públicas (PKI)

É um conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerir, armazenar, distribuir e revogar certificados de chave pública.

É composta por:

- A criação dos pares de chave assimétricas para cada entidade;
- A criação e distribuição dos certificados de chave pública;
- Definição e uso de cadeias de certificados;
- Atualização, publição e distribuição de CRLs;
- Uso de estruturas de dados e protocolos que permitem o funcionamento de serviços;

Tem as seguintes **entidades**:

- **Autoridade de Certificação** (CA): Esta entidade é responsável por emitir, revogar, renovar e gerenciar certificados de chave pública. A CA é crucial para estabelecer a confiança na identidade associada a uma chave pública.

- **Autoridade de Registro** (AR): A AR é encarregada de verificar a identidade dos solicitantes antes que eles possam obter um certificado da CA. A AR age como intermediária entre o usuário e a CA, garantindo que a CA emita certificados apenas para entidades legítimas.

- **Autoridade de Validação** (VA): Em alguns contextos, o termo Autoridade de Validação (VA) pode ser usado para se referir à Autoridade de Certificação (CA). No entanto, em certos sistemas, a VA pode ser uma entidade separada que valida informações específicas sobre os certificados emitidos pela CA.

A PKI define relações de confiança de duas formas diferentes:

- **Emitindo certificados de chave pública de outras CAs**: Hierarquicamente abaixo delas;
- **Requisitando a certificação de chave pública de outras CAs**: Hierarquicamente acima delas;

Estas relações de confiança podem ser:

- **Hierárquicas**: CA raiz e CA intermédias;
- **Cruzadas (cross-certification)**: CA raiz e CA raiz;
- **Em malha (mesh)**: grafos de certificação;

Partilha de segredos

Ver as cenas do fábio e ana...

Provas com conhecimento nulo (ZKP)

Ver as cenas do fábio e ana...

Cifras homomórficas

Uma **cifra homomórfica** é uma cifra que permite que operações matemáticas sejam realizadas sobre os textos cifrados, sem que seja necessário decifrados o texto. Isso permite que os dados sejam processados sem revelar o seu conteúdo, o que é útil em muitos cenários, como a computação em cloud.