Criptografia (MIETI)

Módulo VII – Aplicações: Assinatura Digital

Carlos Bacelar Almeida
jba@di.uminho.pt

Departamento de Informática
Universidade do Minho

S/MIME – Secure/Multipurpose Internet Mail Extensions

- S/MIME oferece uma forma consistente de enviar e receber informação segura no formato MIME (Multipurpose Internet Mail Extensions).
- Disponibiliza os seguintes serviços:
  - autenticação, integridade da mensagem e não repúdio de origem, através da utilização de assinaturas digitais.
  - confidencialidade dos dados, através de da utilização de um esquema de cifra de chave pública (mais precisamente, esquema híbrido).
  - utiliza certificados X509 para autenticação das chaves públicas.
- Standardizado pelo *Internet Engineering Task Force* RFC-5751 (V3.2).
- Suportado pela generalidade das aplicações de EMail (MUA) existentes.

Utilização típica do S/MIME

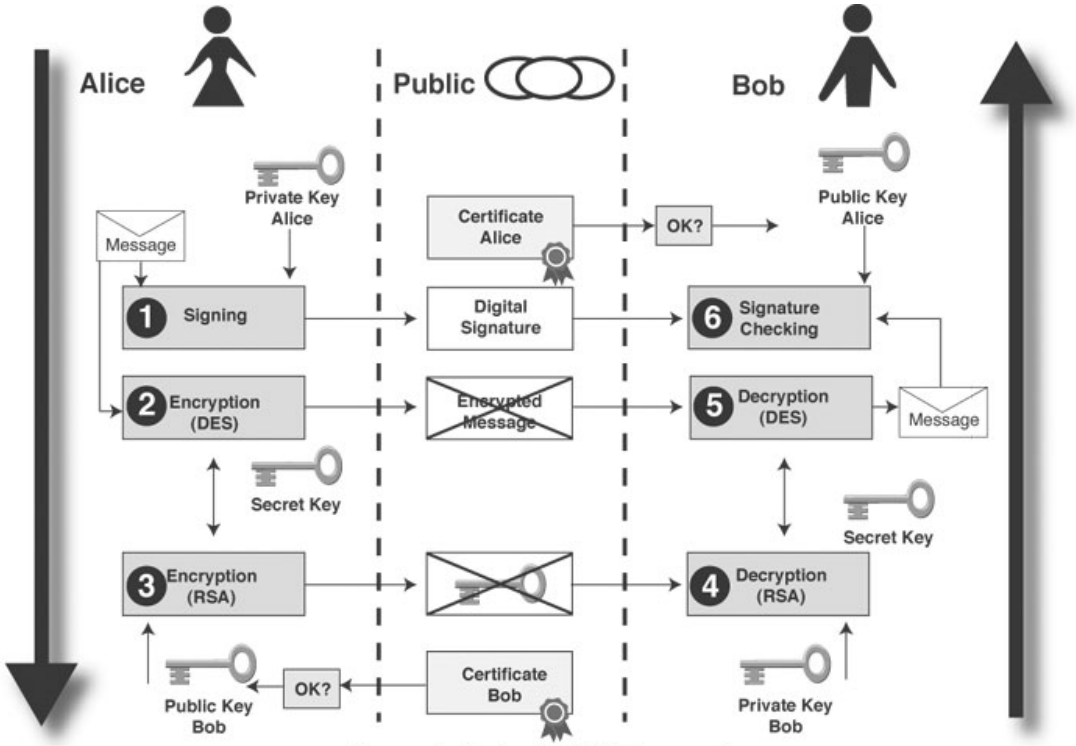


Figure 1: Typical S/MIME scenario

Pretty Good Privacy (PGP)

- O PGP é uma aplicação freeware desenvolvida por Phil Zimmermann com o objectivo de colocar uma infraestrutura para protecção de informação, i.e. privacidade, à disposição do cidadão comum.
- O lançamento deste software causou alguma polémica nos EUA devido às leis que restringiam a difusão e utilização generalizada da chamada *strong cryptography*.
- Até hoje prevalece a ideia, nomeadamente nos EUA, de que a utilização do PGP é ilegal.
- Um argumento apresentado a favor da utilização do PGP, e contra as restrições ao uso de sistemas de protecção da privacidade é: “se a protecção de informação é ilegalizada apenas os fora-da-lei conseguem ter privacidade!”

Funcionamento do PGP

- O PGP é um sistema com três vertentes principais: privacidade, integridade e autenticação, e certificação.
- **Privacidade** Utilização de algoritmos de compressão, cifras simétricas e assimétricas na protecção de informação, nomeadamente ficheiros e mensagens de e-mail.
- **Integridade e Autenticação** Utilização de funções de hash criptográficas e algoritmos de assinatura digital para a assinatura de mensagens e documentos.
- **Certificação** Estabelecimento de relações de confiança e distribuição de chaves públicas com base num esquema certificação próprio, alternativo à PKI e ao X.509.

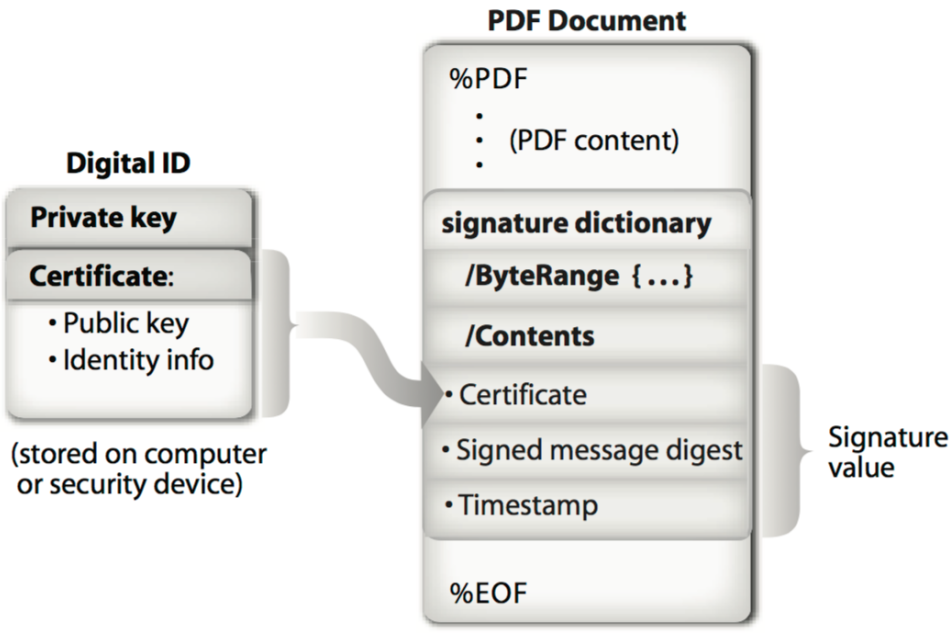
Assinatura de Documentos

- A directiva Europeia Electronic Signature Directive 1999/93/EC vem atribuir estatuto legal à assinatura digital.
  1. Confere em particular, em circunstâncias determinadas, peso legal à propriedade de não repúdio das assinaturas digitais,
  2. ...e equivalência às assinaturas manuscritas em circunstâncias determinadas.
- A directiva define as noções relevantes e estabelece os requisitos necessários e a infra-estrutura de alto nível, mas preserva uma perspectiva neutra em termos de escolhas tecnológicas;
- A concretização do dispositivo ficou a cargo do comité técnico Electronic Signatures and Infrastructures (ESI) do European Telecommunications Standards Institute (ETSI).

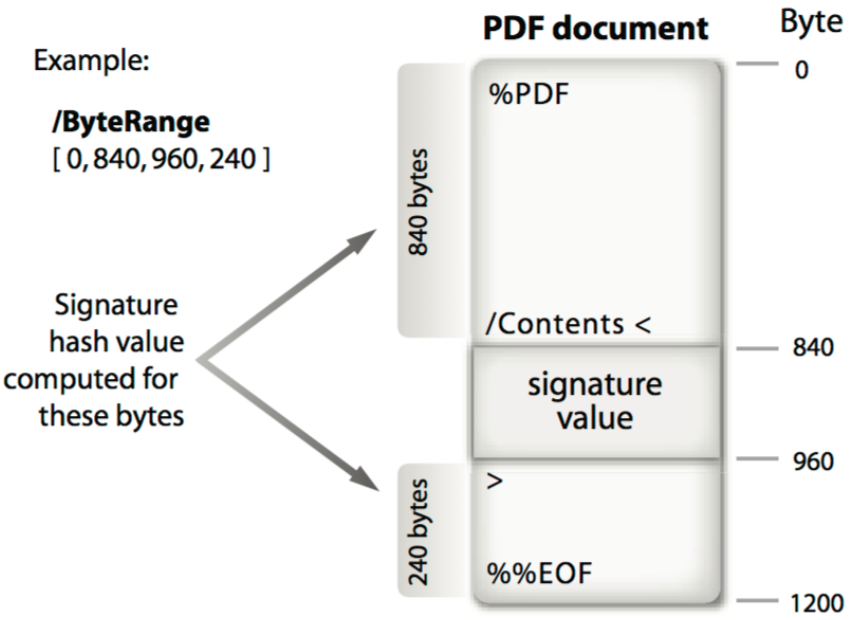
PDF Advanced Electronic Signature (PAdES)

- PDF é um formato que suporta documentos digitais com larga aceitação.
- Originário de uma empresa privada (Adobe), mas entretanto Standardizado por organismos competentes (ISO 32000-1, 32000-2).
- Incluí já suporte a assinaturas digitais (desde V1.7).
- ...o que permite beneficiar das faculdades oferecidas pela assinatura digital com recurso a aplicações disponíveis livremente (e.g. Acrobat Reader).

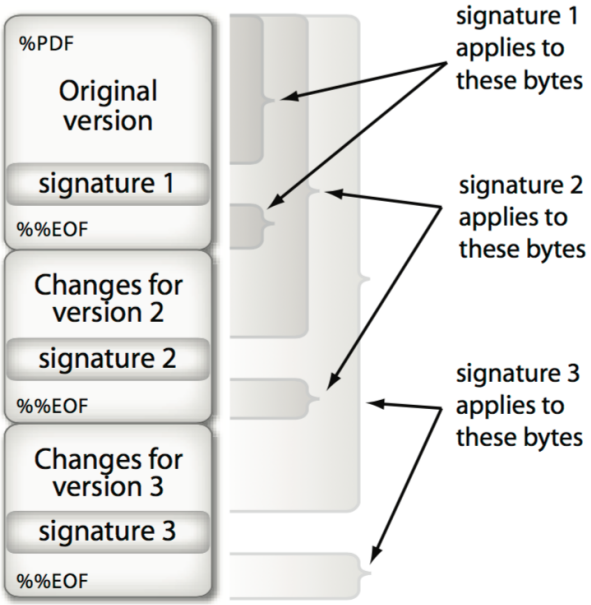
Assinaturas digitais em PDF



- Toda a informação do PDF é considerada para efeitos do cálculo da assinatura.

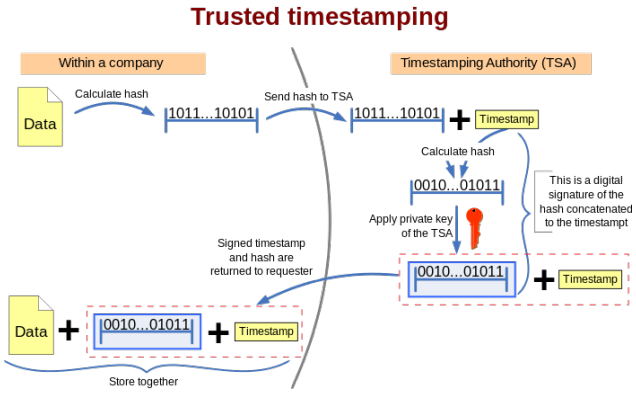


- São suportadas multiplas assinaturas sobre um mesmo documento (assinaturas incrementais).



Autoridades de Timestamping

- Como estabelecer que uma assinatura digital foi realizada num determinado instante?
- Como preservar o facto que, num determinado instante, a assinatura é considerada válida?
- Para ultrapassar essas dificuldades, considera-se uma terceira parte de confiança para atribuir *estampilhas temporais* — **Time-Stamping Authority**.



Parte III

Dispositivos Móveis em Criptografia

Tokens Criptográficos

- Dispositivos electrónicos portáteis que, pela sua natureza, constituem um ambiente protegido para:
  - armazenar informação secreta;
  - executar operações críticas de segurança.
- Disponíveis em diferentes formatos/tecnologias (e.g. USB, bluetooth, smart-card, contactless tokens, ...)
- Normalmente utilizados para autenticação/identificação, ou para realizar operações criptográficas críticas (e.g. assinaturas digitais).
- Chaves criptográficas podem ser *geradas*, *armazenadas*, e *utilizadas* no prórpio dispositivo.
- Incluem normalmente medidas de protecção físicas (*tamper resistant packaging*)

Cartão de Cidadão

- Cartão que concentra informação antes dispersa por:
  - Bilhete de Identidade
  - Cartão de Contribuinte
  - Cartão de Eleitor
  - Cartão da Segurança Social
  - Cartão de utente do Serviço Nacional de Saúde
- *Smart-card* com funcionalidades criptográficas, contendo informação em formato digital do utente:
  - Números de identificação (BI, Contribuinte, ...)
  - Dados publicos (data de validade, nome, data nascimento, sexo, ...)
  - Dados biométricos (fotografia

Características

- Como documento físico o cartão de cidadão permite ao respectivo titular provar a sua identidade perante terceiros através da leitura de elementos visíveis (possivelmente coadjuvada pela leitura óptica de uma zona específica).
- Como documento digital o cartão de cidadão permite ao respectivo titular
  - provar a sua identidade perante terceiros através de autenticação electrónica.
  - autenticar de forma unívoca através de uma assinatura electrónica qualificada a sua qualidade de autor de um documento electrónico.
- Serviço *Fornecedor de Autenticação* disponibiliza uma plataforma de autenticação centralizada que possibilita a inteoperabilidade de diferentes entidades na esfera da função pública (e.g. Portal do Cidadão, Portal do cliente bancário, ...)

Funcionalidades Criptográficas

- Dois certificados pessoais com respectivas chaves privadas
  - autenticação
  - assinatura qualificada
- Certificados das CAs da cadeia de certificação
- Coprocessador criptográfico (RSA)
- Assinaturas realizadas no próprio cartão (chaves privadas protegidas por PIN)
- Outras chaves para acesso privilegiado (e.g. serviços de segurança)