

Assinatura Digital

Assinatura Digital e novo regime
da Peças Processuais a Juízo



Paulo Trezentos
ADETTI / ISCTE
05/04/2003 – Caldas da Rainha

Agenda

- Alguns conceitos
- Assinaturas digitais
- Certificação e entidades certificadoras
- Segurança dos dados
 - WebSites
 - Correio electrónico

A Assinatura Digital

2

Internet e suas aplicações (âmbito advocacia)

- Consulta de legislação on-line
- Compras on-line
- ...



- Envio peças processuais
- Comunicação com clientes
- Comunicação com colegas
- ...

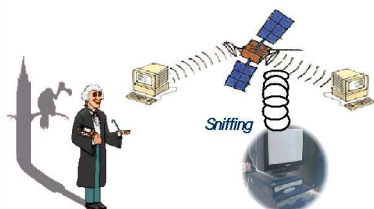
1 / 1 / 2003
Artigo 150.º2

Ameaças I (Web)



Perigo:
- Apropriação de informação
- Prestar informações falsas

Ameaças II (Web)



Perigo:
- Apropriação de informação
- Interna ou externa à organização

Soluções (Web)

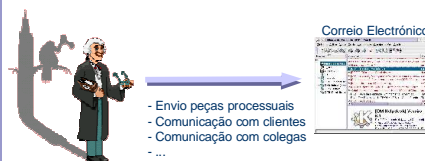
- Utilização de browser com SSL (cliente)
- Não fazer transacções de informação se o *sítio* não suportar SSL
- Como identificar:



SSL – Secure Socket Layer

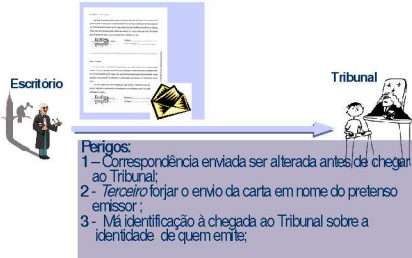
- SSL – Secure Sockets Layer
 - Encriptação da comunicação
 - Autenticação do servidor
 - Utilização de um encriptação assimétrica RSA (chave pública)

Correio Electrónico



- Envio peças processuais
- Comunicação com clientes
- Comunicação com colegas
- ...

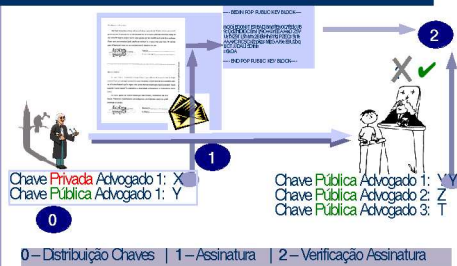
Ameaças I (Correio Electrónico)



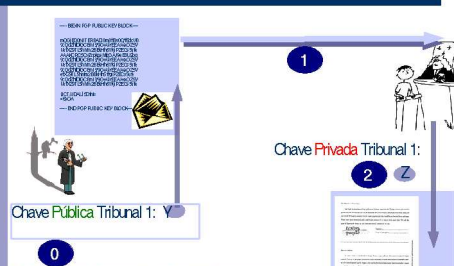
Solução: Assinatura digital

- Três funções:
 - Autenticação
 - Não repúdio
 - Integridade
 - e ainda: confidencialidade
- Tecnologia
 - RSA – encriptação assimétrica
 - Chave pública e chave privada
 - 25 anos

Assinatura Digital : Processo



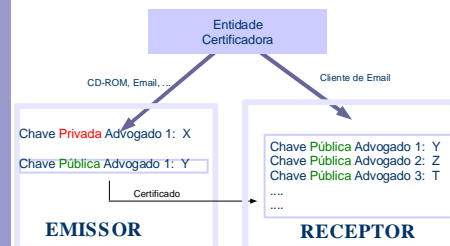
Encriptação



Terminologia

- Assinatura digital
- Public Key Infrastructure (PKI)
- Entidade certificadora (MultiCert, Certipor, GlobalSign, ...)
- Certificado digital
- Chave pública / chave privada
- Norma X.509

Distribuição de Chaves (PKI)



Vantagens da Assinatura Digital

- **Nível de segurança** superior assinatura tradicional
- **Flexibilidade:** possível associar diferentes tipos documentos
- **Facilidade de transmissão:** via digital (+ rápido e barato)
- **Facilidade de confirmação** da autenticidade e integridade
- **Não repudição**

Desvantagens da Assinatura Digital

- Possibilidade de **roubo / extravio** da chave privada
- Legalmente ainda sem aceitação universal
- Sistema de **distribuição de chaves** (PKI) complexo
- **Quebra do algoritmo** / evolução da capacidade de processamento

Ameaças à chave privada

- **Roubo “clássico”**
 - Terceiro introduz-se no computador e retira a chave privada
- **Prevenção:**
 - *password complexa*
 - acesso físico ao computador
 - Utilização de smart cards

Ameaças à chave privada II

- **Extravio**
 - **Prevenção:** ter uma cópia de segurança em suporte externo ao computador
 - Mudança de email
- **Quebra do algoritmo**
 - Matematicamente
 - Pela evolução do poder computação

Quebra do algoritmo

- Depende do tamanho da chave pública
 - **256 bits** – facilmente quebrável
 - **384 bits** – universidades e grupos de investigação
 - **512 bits** – NSA? Alguns governos... (1999)
 - **768 bits** – Segura a curto termo
 - **1024 bits** – Segura no futuro imediato
 - **2048 bits** – Segura por décadas?
- Chave tem de expirar ...

Conclusões

- Web e o Correio electrónico poderão tornar-se poderosas ferramentas
- Software totalmente preparado
- Legislação abrangente
- Logicamente tem de existir alguma evolução na infra-estrutura de distribuição de chaves e das entidades certificadoras



Obrigado.

Perguntas / comentários ?

Paulo Trezentos
Paulo.Trezentos@iscte.pt