apdsi
associação para a promoção e desenvolvimento da Sociedade da Informação

Certificação Digital - Será Que é Para Valer?

29 | abril | 2015
Auditório
Escola Profissional Gustave Eiffel

Apoio Institucional

Patrocinadores Globais

A Certificação Digital numa Sociedade Desmaterializada

Pedro Veiga

www.ciencias.ulisboa.pt

Certificação Digital

- Assegurar a autenticidade da informação digital

Uso da Certificação Digital

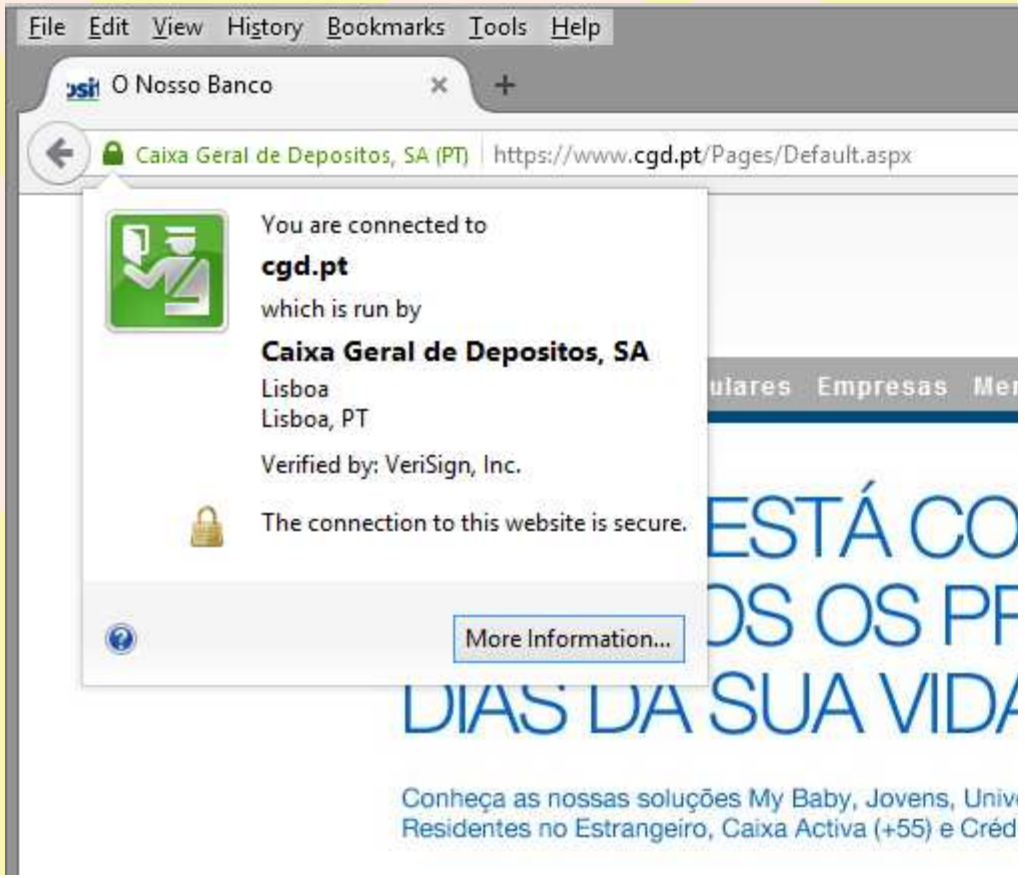
- Certificação de documentos
- Certificação de entidades
- Certificação de hardware
- Certificação de Software
- Certificação de Computadores

Certificação de Computadores

- Como sei que o computador a que me ligo é aquele a que me quero ligar?
- DNSSEC
- Certificados Digitais

Certificação de Computadores

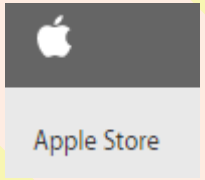
- Como sei que o computador a que me ligo é aquele a que me quero ligar?
- DNSSEC
- Certificados Digitais



Certificação de Software

- Como confio no software que instalo no meu computador?

- E na AppleStore

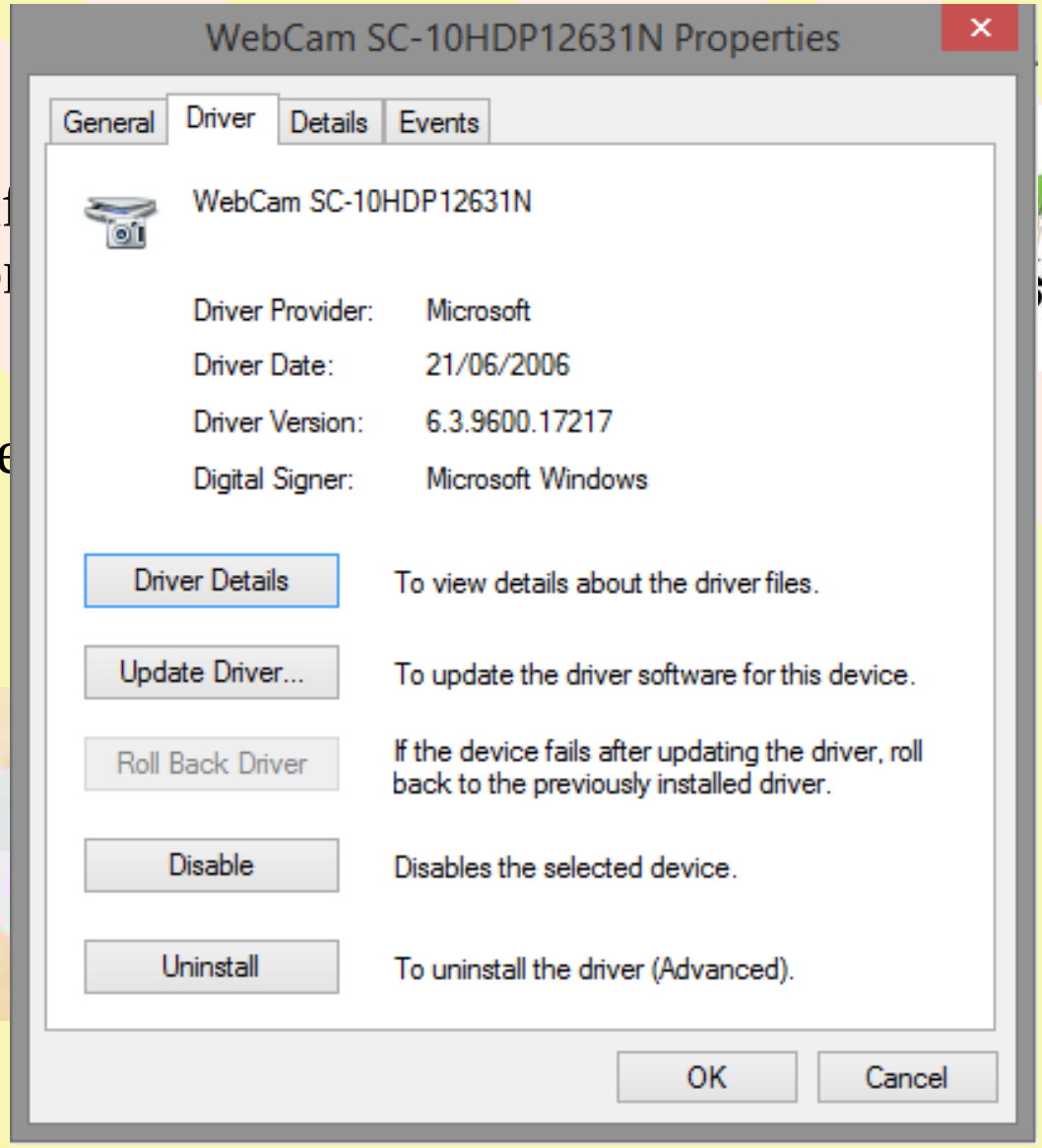


- E na

E se é SW 3rd Party?

Certificação de Software

- Como conf
  no meu co
- E na Apple
- E na

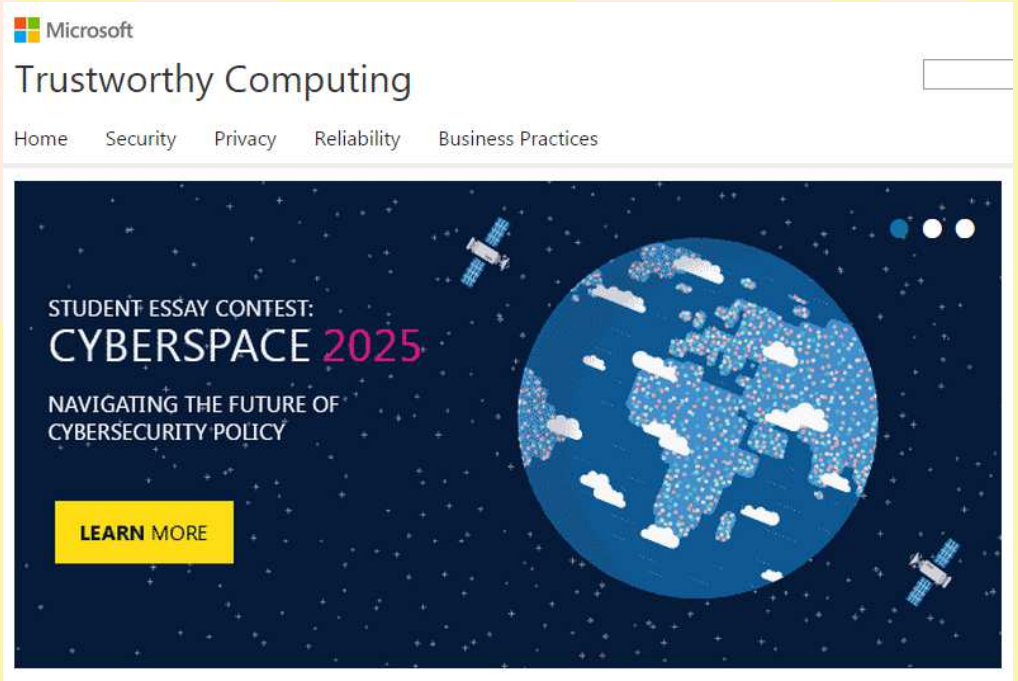


3rd Party?

Certificação de Hardware

- Importante mas falamos de outra vez ☹ ☺

- Trustworthy Computing



Certificação de entidades

Introdução à Criptografia

- Técnica que consiste em transformar os dados a transmitir de modo a inviabilizar o seu uso, em tempo útil, se forem interceptados

- Se M é a mensagem a transmitir

- M’ = F(M, K_1)
- M = F(M’, K_2)

- Sem saber K_1 ou K_2 é “impossível” recuperar M a partir de M’

Criptografia

- Criptografia simétrica
  - K_1 e K_2 são iguais (K)
  - Capacidade do sistema depende de manter K confidencial
  - Computacionalmente pouco exigente
- Criptografia assimétrica
  - K_1 e K_2 são diferentes
  - K_1 e K_2 são intermutáveis
    - » Uma das chaves chama-se chave privada e a outra chave pública
  - Computacionalmente mais exigente
- Sem saber K_1 ou K_2 é “impossível” recuperar M a partir de M’

Assinar Documentos

- A assinatura autógrafa

- Assinatura Electrónica

e

- Assinatura Digital

Algumas Definições

- Integridade
  - O receptor de uma mensagem poder verificar se esta foi, ou não, adulterada
- Autenticação dos utilizadores
  - Cada elemento envolvido numa troca de mensagens poder verificar a identificação do emissor e/ou do destinatário
- Não repudiação
  - O emissor de uma mensagem não poder negar que a enviou
- Assinatura Digital
  - Adição de informação a uma mensagem para garantir a sua autoria

Assinatura Digital

- Fase 1
  - Produzir documento
  - Gerar o seu sumário
- Fase 2
  - Enviar documento
  - Enviar sumário cifrado com chave privada do emissor
- Fase 3
  - Receber documento
  - Gerar sumário e compará-lo com sumário recebido (depois de decifrado com a chave pública do emissor)

- E se pretender que o documento seja confidencial?

Certificados X.509

- Tecnologia para fazer a gestão de chaves privadas de entidades
- Estrutura de dados que inclui:
  - Chave privada
  - Elementos que ajudam à gestão dos certificados

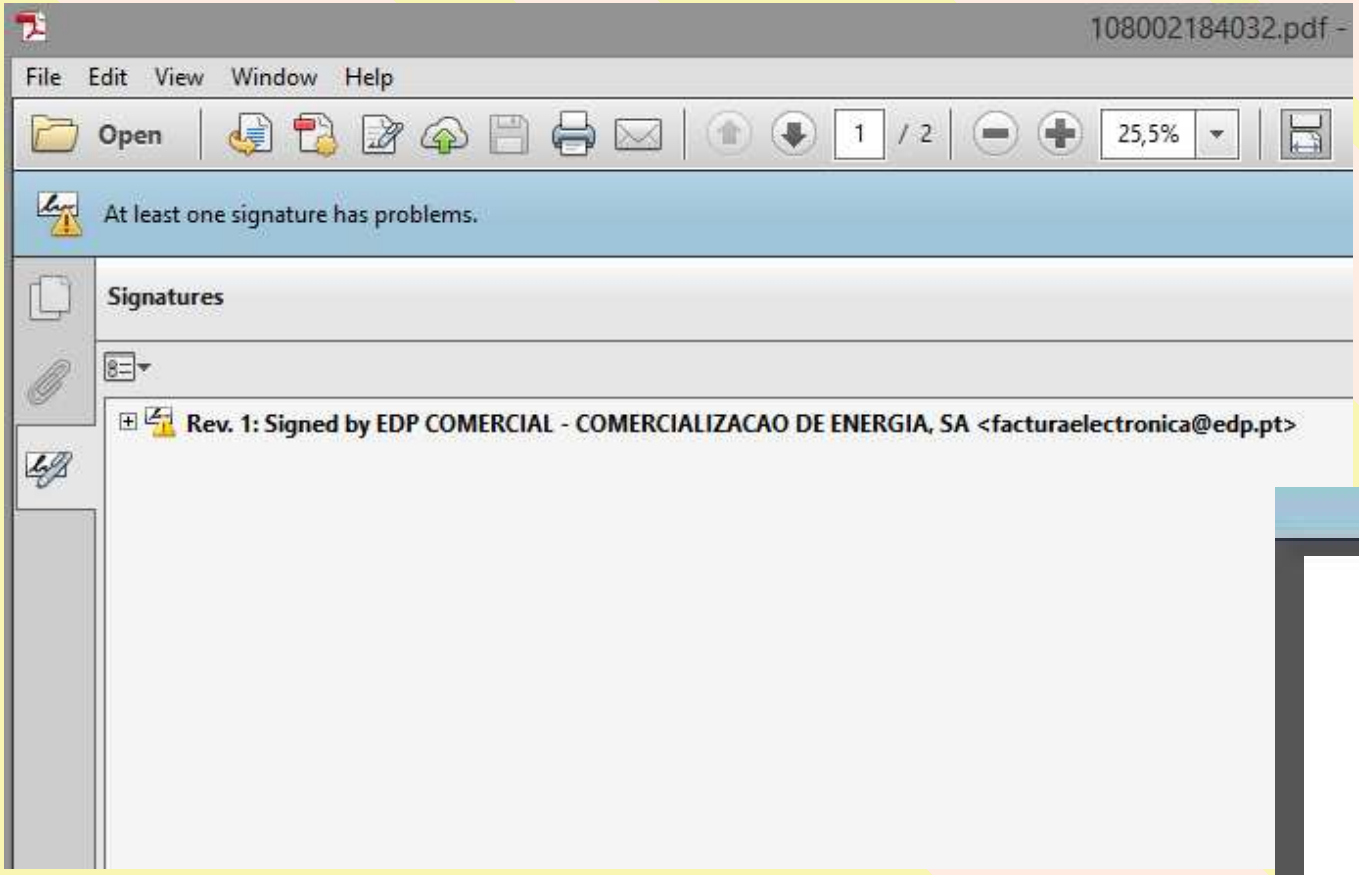
Estrutura de Certificado X.509 v3

- Certificate
  - Version
  - Serial Number
  - Algorithm ID
  - Issuer
  - Validity
    - » Not Before
    - » Not After
  - Subject
  - Subject Public Key Info
    - » Public Key Algorithm
    - » Subject Public Key
  - Issuer Unique Identifier (optional)
  - Subject Unique Identifier (optional)
  - Extensions (optional)
    - » ...
- Certificate Signature Algorithm
- Certificate Signature

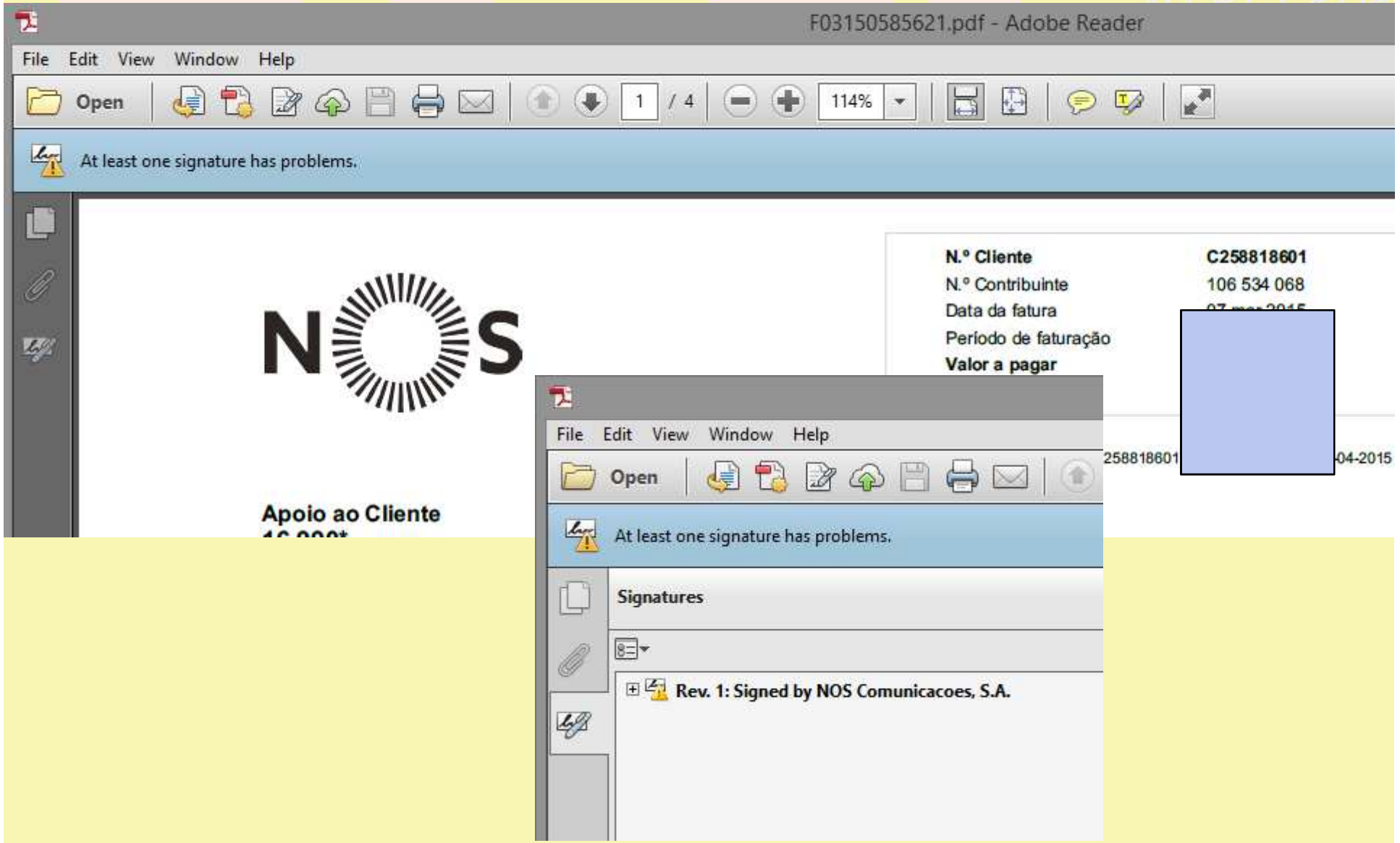
PKI – Public Key Infrastructure

- Autoridade de certificação
- Organização que faz gestão de utilizadores e dos respectivos certificados
- Plataforma tecnológica de geração de pares de chaves
  - Chaves privadas e sua entrega segura
  - Chaves públicas e sua disponibilização
- Gestão da segurança
  - Chaves perdidas, comprometidas
  - Colocação de certificados de raiz em aplicações comuns

Certificação de documentos



Certificação de documentos



Notas Finais

- Tecnologia há
- Enquadramento legislativo há
- Vontade de mudar … não há!
  - Ignorância?
  - Inércia?