



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



accenture

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

NOS

ORACLE



everis
an NTT DATA Company

Quidgest

UNISYS



**Ciências
ULisboa**

**Internet
Society**

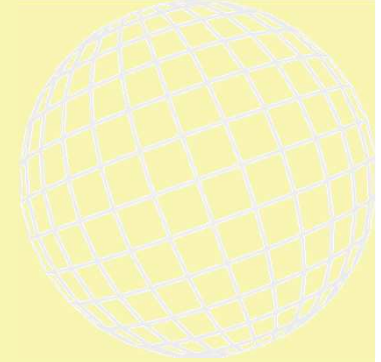


Portugal Chapter

A Certificação Digital numa Sociedade Desmaterializada

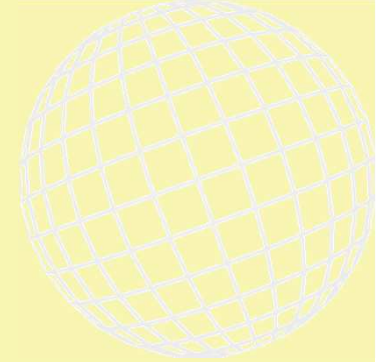
Pedro Veiga
www.ciencias.ulisboa.pt

Certificação Digital

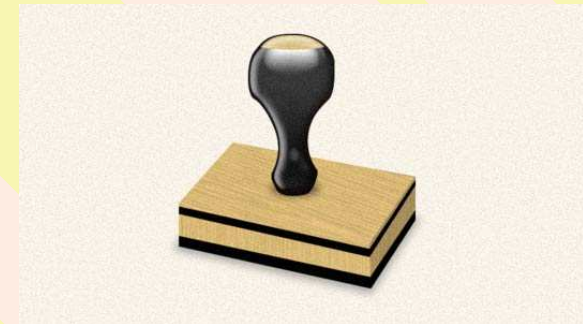


- Assegurar a autenticidade da informação digital

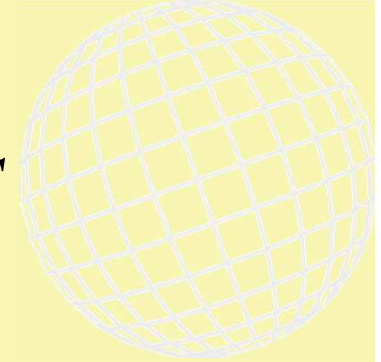
Uso da Certificação Digital



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



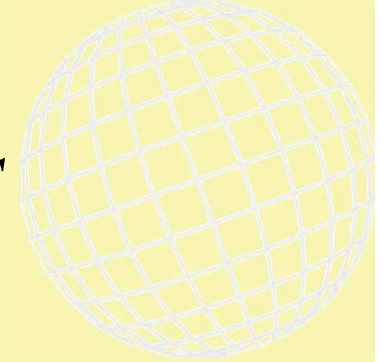
Certificação de Computadores



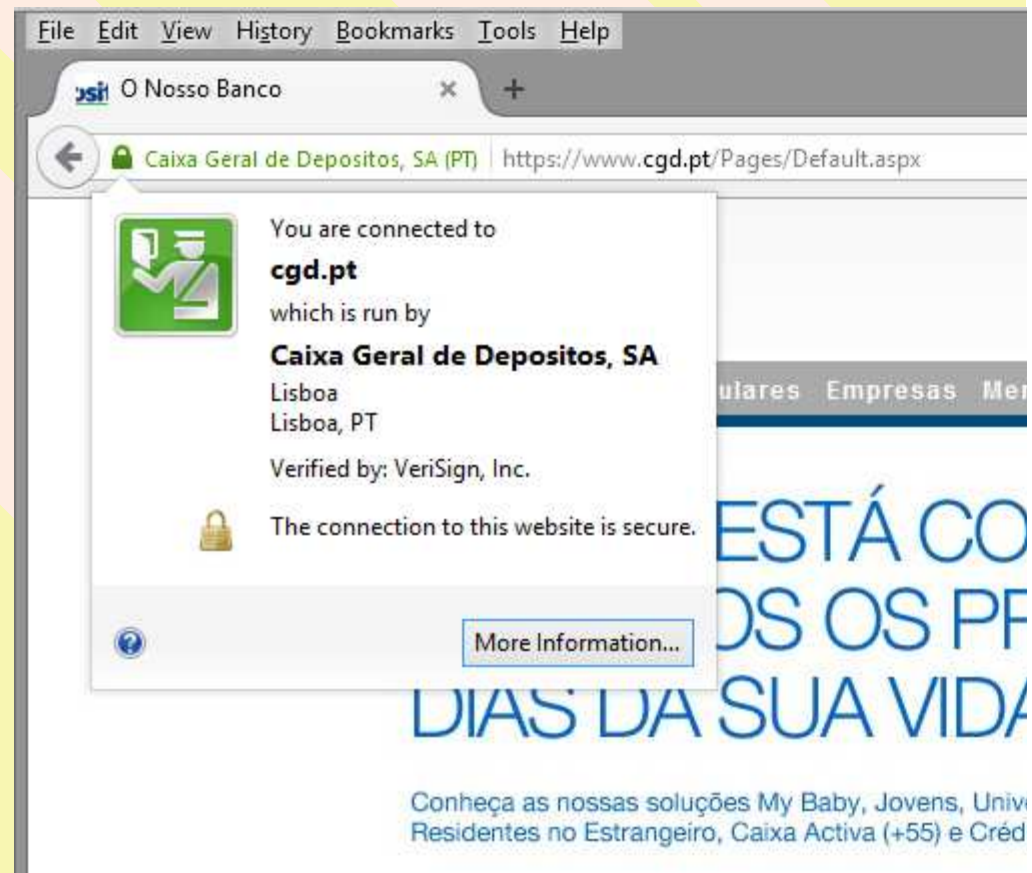
- Como sei que o computador a que me ligo é aquele a que me quero ligar?
- DNSSEC
- Certificados Digitais

The screenshot shows the website of Caixa Geral de Depósitos (CGD) in Portuguese. The browser address bar shows the URL <https://www.cgd.pt/Pages/Default.aspx>. The main banner features the text "UMA COISA É CERTA, DESTA NÃO TE VAIS ESQUECER. A CAIXA LEVA-TE AOS FESTIVAIS DE VERÃO" with a "SABE COMO" button. Below the banner are navigation tabs for "O Nosso Banco", "Particulares", "Empresas", and "Mercados". A sidebar on the left lists services like "Espaço Cliente", "Segurança", "Recrutamento", and "Incumprimento - Prevenção". The main content area is divided into sections for "EMPRESAS" and "PARTICULARES", each with a featured article and a world map icon.

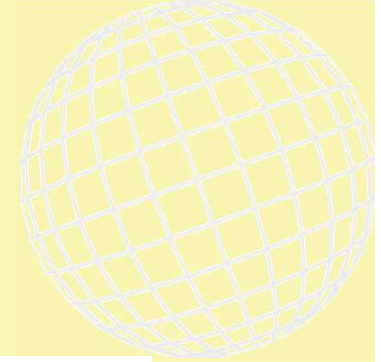
Certificação de Computadores



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



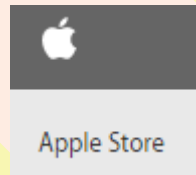
Certificação de Software



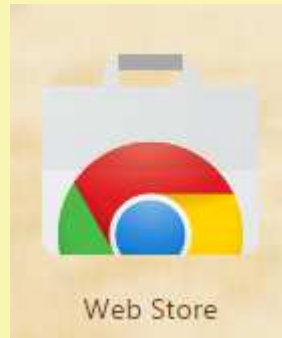
- Como confio no software que instalo no meu computador?



- E na AppleStore



- E na



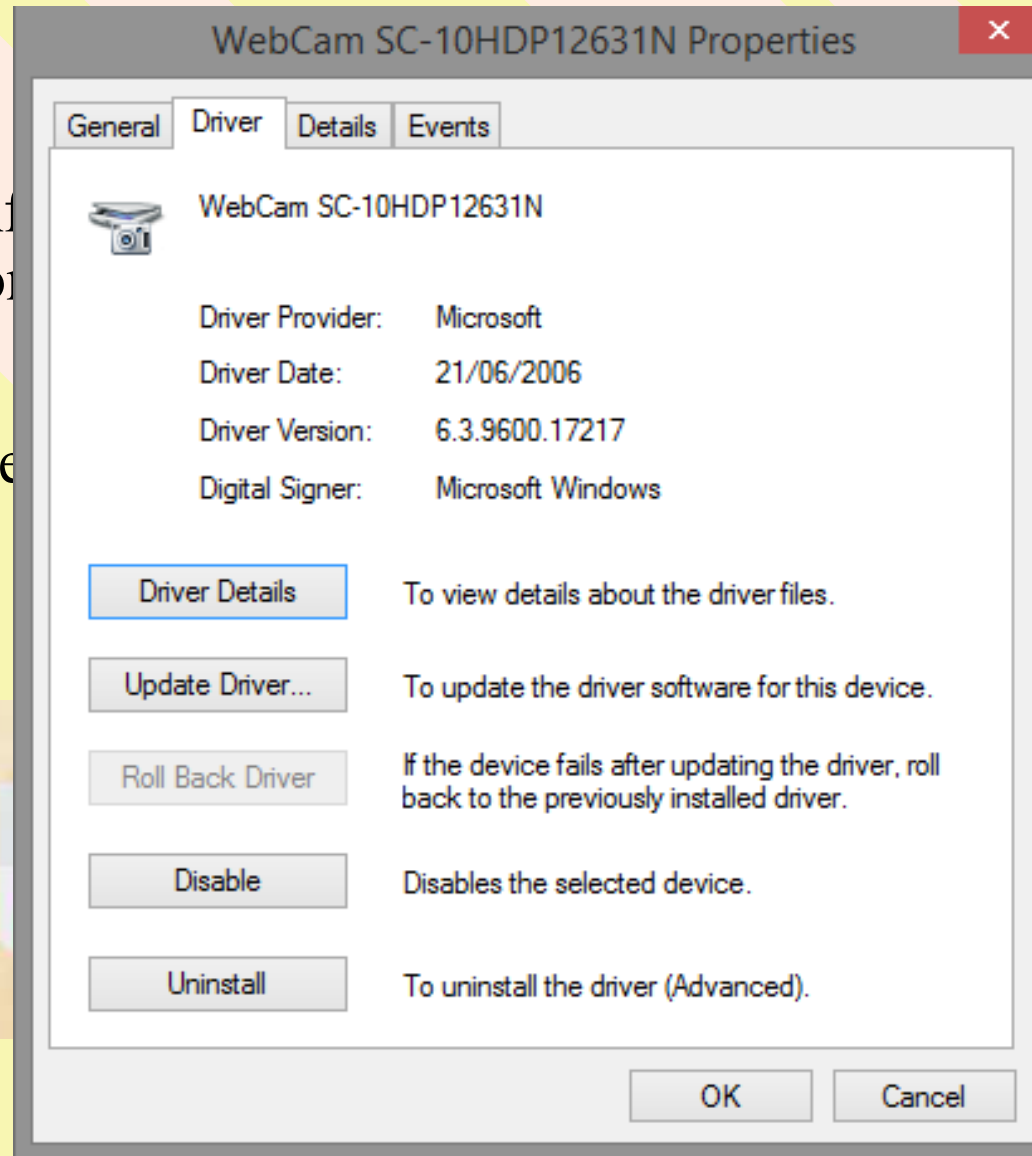
E se é SW 3rd Party?

Certificação de Software

■ Como funciona no meu computador?

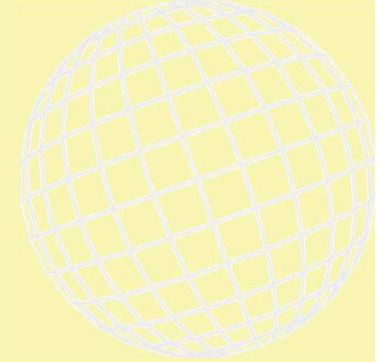
■ E na Apple?

■ E na



3rd Party?

Certificação de Hardware



■ Importante mas falamos de outra vez ☹️ 😊

■ Trustworthy Computing

Microsoft
Trustworthy Computing

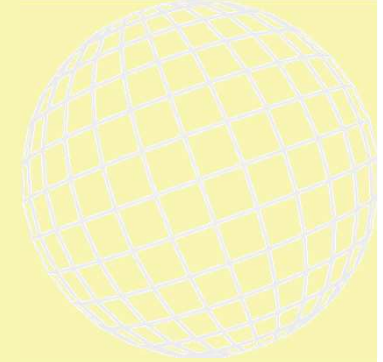
Home Security Privacy Reliability Business Practices

STUDENT ESSAY CONTEST:
CYBERSPACE 2025

NAVIGATING THE FUTURE OF
CYBERSECURITY POLICY

LEARN MORE

Certificação de entidades





ESTADO DE BRASÍLIA
ESTRELA VERDE

PORTUGAL

FELETEROS-SACRAMENTO DOS SANTOS FONSECA
VISCONDELOS DE BRAGANÇA

ISABEL MARIA LUISA GABRIELA PALA B

F 179 - PPT 12/11/1988

01234567 2A3 1234567





PORTUGAL

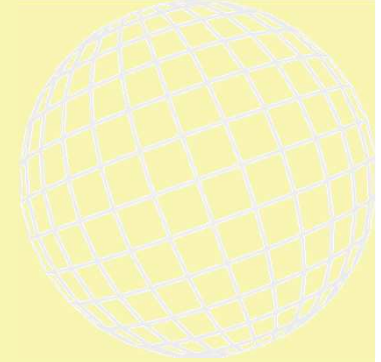
ANTÓNIO JORGE MANUEL SILVA LOPES ALUM DOS SANTOS
FONSECA VISCONDELOS - ANA MARGARIDA LUISA MATEUS
DOS SANTOS FONSECA VISCONDELOS

200901430
01800094500
90090438

```

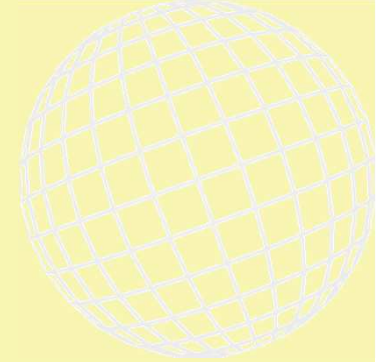
I<PRT01234567<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
7106118F003134PRT<<<<<<<<<<<<<<<<<<<<<
BRAGANCA<<ISABEL<MARIA<<<<<<<<
                
```

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

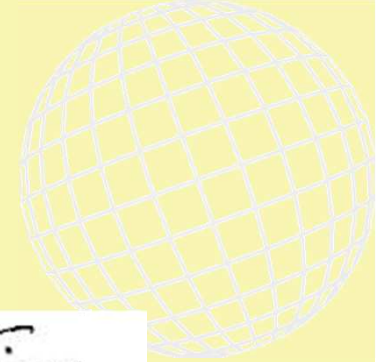


- **Criptografia simétrica**
 - K_1 e K_2 são iguais (K)
 - Capacidade do sistema depende de manter K confidencial
 - Computacionalmente pouco exigente

- **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



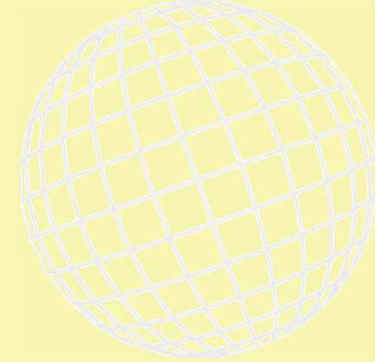
- Assinatura Electrónica



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

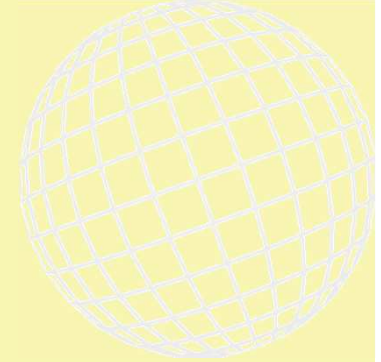
■ Não repudição

- O emissor de uma mensagem não poder negar que a enviou

■ Assinatura Digital

- Adição de informação a uma mensagem para garantir a sua autoria

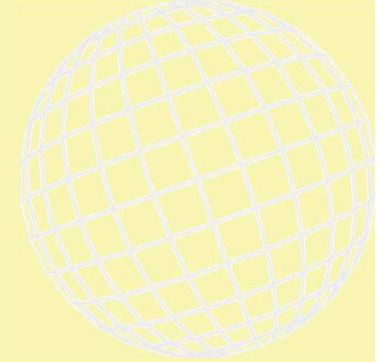
Assinatura Digital



- 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?

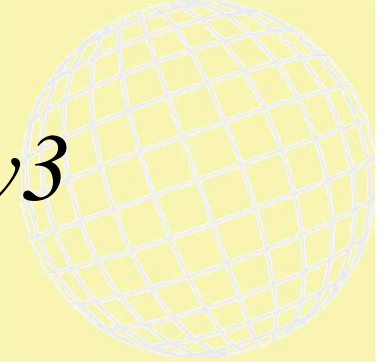
Certificados X.509



- 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



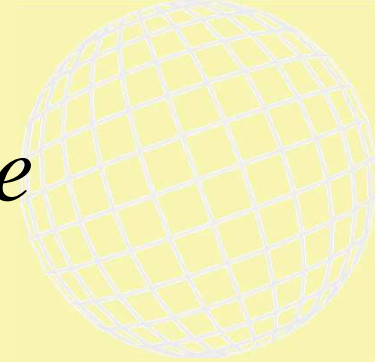
■ Certificate

- 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

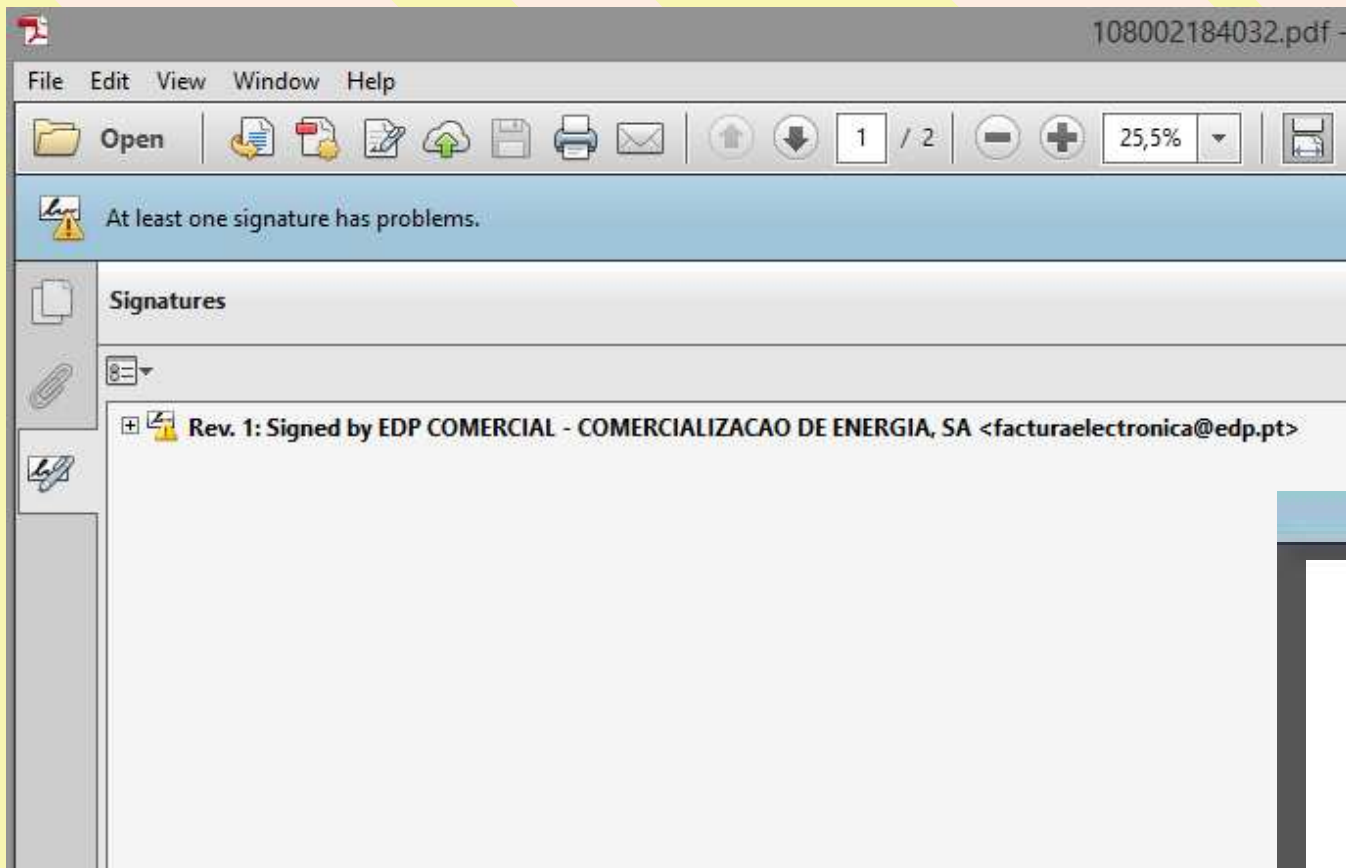
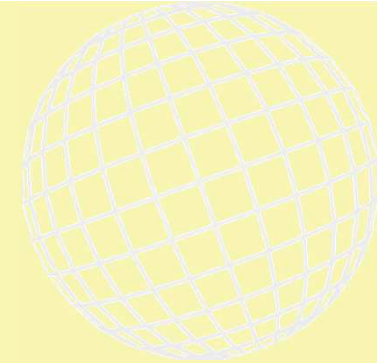
■ Certificate Signature

PKI – Public Key Infrastructure

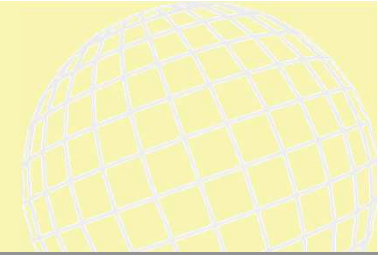


- Autoridade de certificação
- Organização que faz gestão de utilizadores e dos respectivos certificados
- Plataforma tecnológica de geração de pares de chaves
 - Chaves privadas e sua entrega segura
 - Chaves públicas e sua disponibilização
- Gestão da segurança
 - Chaves perdidas, comprometidas
 -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

Certificação de documentos



Certificação de documentos



The screenshot shows the Adobe Reader interface with a PDF document titled "F03150585621.pdf". The document content includes the NOS logo and a table of invoice details. A signature error message is displayed at the top of the document area. A "Signatures" panel is open, showing a list of signatories.

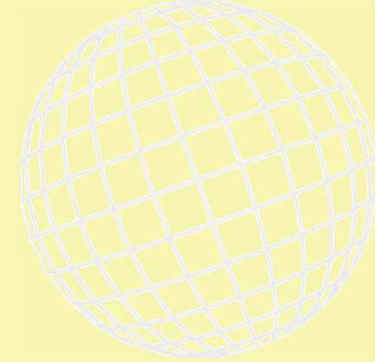
Field	Value
N.º Cliente	C258818601
N.º Contribuinte	106 534 068
Data da fatura	07 mar 2015
Período de faturação	
Valor a pagar	

At least one signature has problems.

Signatures

- Rev. 1: Signed by NOS Comunicacoes, S.A.

Notas Finais



- Tecnologia há

- Enquadramento legislativo há

- Vontade de mudar ... não há!
 - Ignorância?
 - Inércia?