

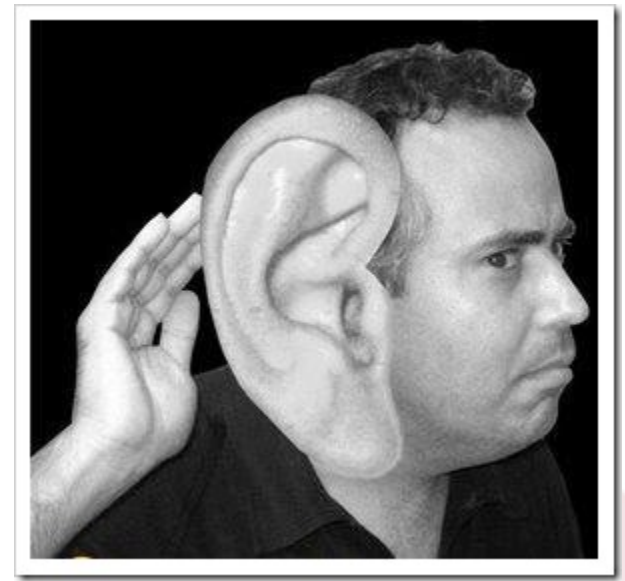
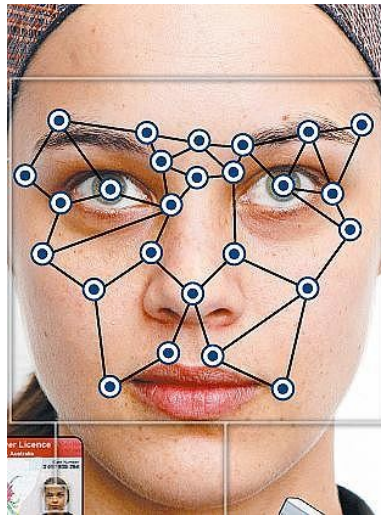
Assinaturas digitais qualificadas com o Cartão de Cidadão



Definições

- **Autenticação**
 - capacidade de garantir que uma entidade é quem afirma ser

Autenticação – Mundo real



Autenticação – Informática

- Segredo
 - Senha
- Algo que possuímos
 - Token criptográfico
- Algo que somos
 - Dados biométricos
 - Impressão digital
 - Íris, Voz, face



Chip
criptográfico



Definições

- **Não-repúdio**
 - capacidade de impedir que uma entidade negue a sua participação numa transação

Não-repúdio – Mundo real

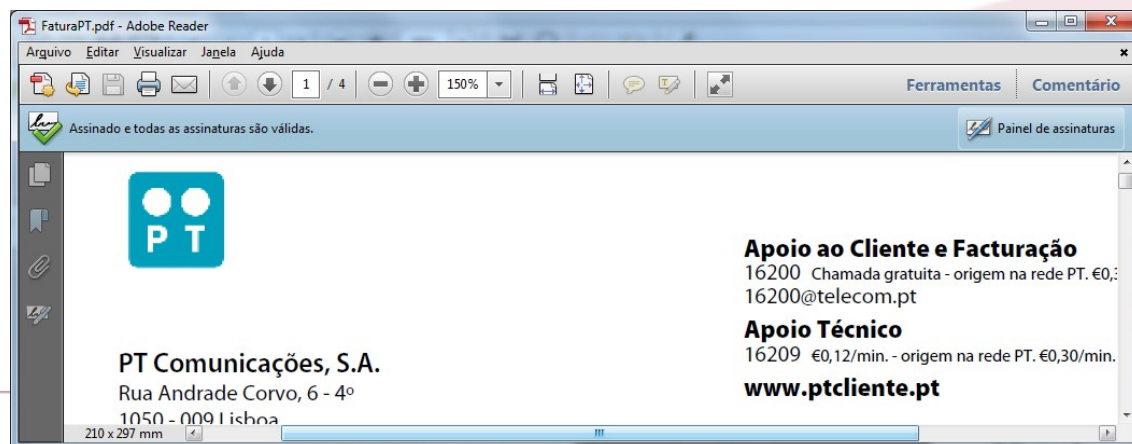
- Assinaturas (em alguns casos têm de ser presenciais)



Francisco Campos

Não-repúdio – Informática

- Assinaturas electrónicas qualificadas
 - Pessoais: com cartão do cidadão
 - Documentos, emails, ...
 - Empresas: ex. facturas, ...



- Assinaturas digitais
 - O que são?
 - Como funcionam?
 - Qual é a sua validade legal?
 - Como se faz uma assinatura digital?

Conceitos

- Assinaturas digitais
 - Mecanismo criptográfico que permite garantir o não-repúdio
- Não confundir:
 - Assinaturas digitalizadas
 - Assinaturas electrónicas
 - Assinaturas digitais
- Embora parecidos, têm significados e validade legais diferentes.

Assinaturas digitalizadas

- Conversão de uma assinatura manuscrita em suporte físico (ex. papel) para uma imagem em suporte digital (ex. ficheiro)
 - Muito fácil de copiar
 - Sozinha não dá garantias de não-repúdio
 - Exemplo de utilização: Fax



Francisco Campos

Assinaturas electrónicas

- Definição legal (Decreto-Lei 62/2003):
 - **Assinatura electrónica**: resultado de um processamento electrónico de dados susceptível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico;
 - **Exemplo**: simples escrita do nome completo para identificar o remetente de um documento electrónico (email, .doc, pdf, etc)

Assinaturas electrónicas

- Definição legal (Decreto-Lei 62/2003):
 - **Assinatura electrónica avançada**: assinatura electrónica que preenche os seguintes requisitos:
 - Identifica de forma unívoca o titular como autor do documento;
 - A sua aposição ao documento depende apenas da vontade do titular;
 - É criada com meios que o titular pode manter sob seu controlo exclusivo;
 - A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste;
 - **Exemplo**: assinaturas arbitradas: www.hellosign.com e www.eevid.com
 - Neste contexto as assinaturas digitalizadas são válidas

Assinaturas electrónicas

- Definição legal (Decreto-Lei 62/2003):
 - **Assinatura digital**: modalidade de assinatura electrónica avançada baseada em **sistema criptográfico** assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e **se o documento electrónico foi alterado depois de aposta a assinatura**;
 - **Exemplo**: email com certificados digitais em ficheiros

Assinaturas electrónicas

- Definição legal (Decreto-Lei 62/2003):
 - **Assinatura electrónica qualificada**: assinatura digital ou outra modalidade de assinatura electrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas **através de um dispositivo seguro de criação de assinatura**;
 - Nem todas as assinaturas digitais são qualificadas
 - **Exemplo**: assinaturas digitais com cartão de cidadão

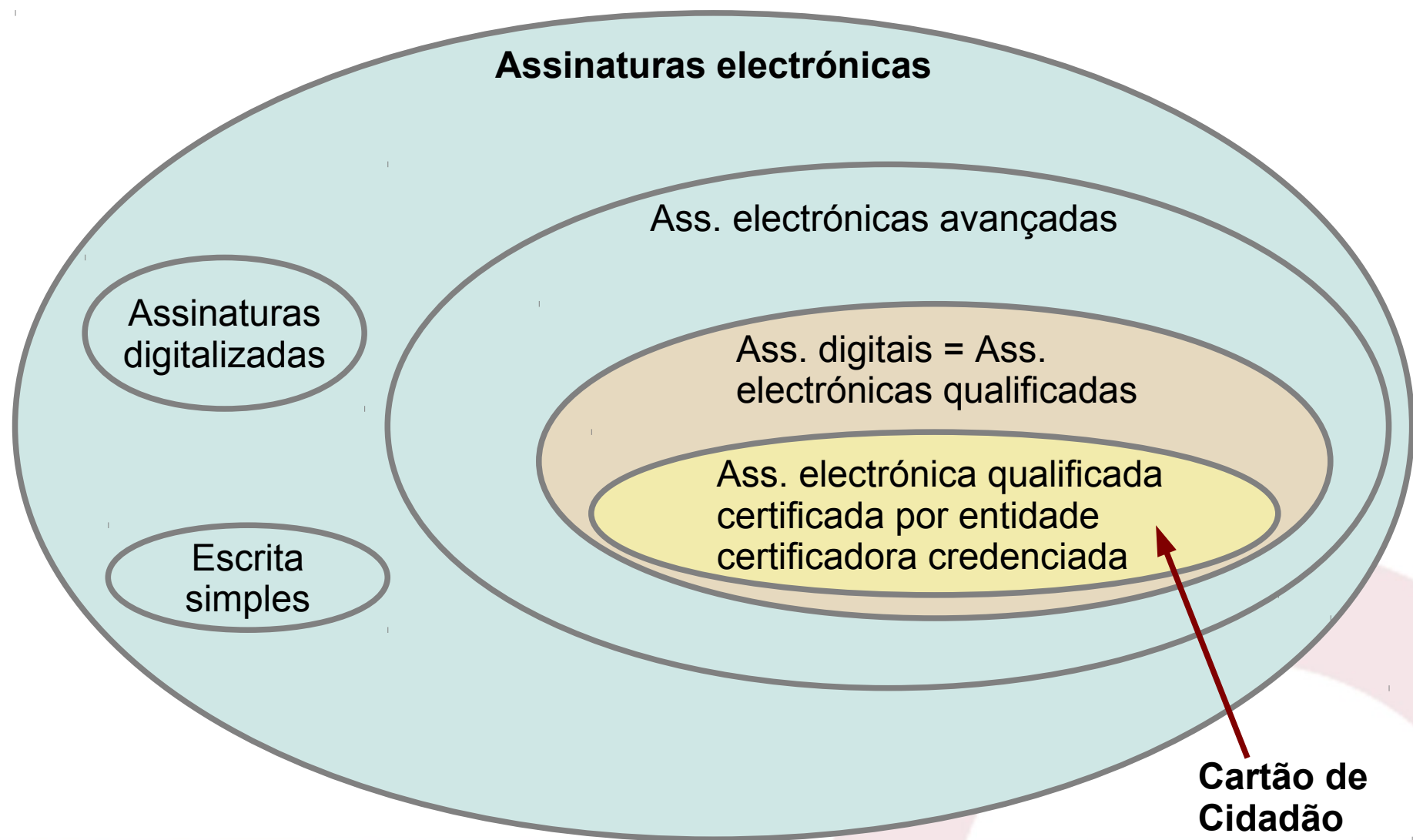
Assinaturas electrónicas

- Definição legal (Decreto-Lei 62/2003):
 - **Dispositivo seguro de criação de assinatura**: dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que:
 - Os **dados necessários à criação de uma assinatura** utilizados na geração de uma assinatura **só possam ocorrer uma única vez** e que **a confidencialidade desses dados se encontre assegurada**;
 - Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e **que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis**;

Assinaturas electrónicas

- Definição legal (Decreto-Lei 62/2003):
 - Dispositivo seguro de criação de assinatura:
(continuação)
 - Os **dados necessários à criação de uma assinatura** utilizados na geração de uma assinatura possam ser eficazmente **protegidos pelo titular contra a utilização ilegítima por terceiros**;
 - Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura;

Assinaturas Digitais



Assinaturas com Cartão de Cidadão (DL 62/2003)

- **Assinatura electrónica qualificada certificada por entidade certificadora credenciada**
 - **Assinatura electrónica qualificada** → já falámos
 - **certificada por entidade certificadora** → uma 3ª entidade (conhecida como entidade certificadora, ou CA) que certifica a identidade (certificados digitais, norma x.509)
 - **credenciada** → essa 3ª entidade legalmente autorizada e reconhecida para emitir identidades digitais: **entidade credenciadora**
 - Em Portugal, o organismo que exerce essa função é a Autoridade Nacional de Segurança (ANS) DL 116-A/2006

Porque é que o sistema das assinaturas com cartão de cidadão é tão complexo?

- Sistema baseada em criptografia assimétrica
- Tipos de cifra:
 - Simétrica – a mesma chave para cifrar e decifrar
 - Troca-se de chave regularmente (duração \leq 1 dia)
 - Assimétrica – a chave que cifra é diferente da chave que decifra
 - As chaves identificam entidades, permanecem as mesmas por longos periodos (duração: 1 a 5 anos)

Criptografia assimétrica e o DL 62/2003

- Terminologia tecnologicamente neutra
- Criptografia assimétrica:
 - Chave privada (não pode ser divulgada) → dados de criação de assinatura
 - Chave pública (deve ser divulgada) → dados de validação de assinatura
 - Assinatura digital → Ass. electrónicas qualificadas
- No DL não existe referência à cifra de dados
 - Porque o CC não o permite fazer (infelizmente)

Certificados digitais

- As chaves públicas
 - São um conjunto grande de bits ≥ 1024 bits
 - Sozinhos não permitem identificar ninguém
 - É necessário **adicionar informação da identidade** (ID) do dono da chave pública
- Como adicionar o ID?
 - ID + Chave pública
 - Não é seguro, é facilmente forjado
 - Certificados digitais (x.509)
 - ID + Chave pública + T + assinatura da EC

Como se validam assinaturas?

- Com o certificado digital (chave pública) de quem assinou
- E com o certificado digital da EC que assinou o certificado digital
- E quem assina o certificado da EC?
 - Outra EC (cadeia)
 - Ou ela própria (auto assinado)
 - Ela própria? Mas isso é de confiança?
 - » Se for credenciada sim.

Como se validam assinaturas?

- Como é que obtemos os certificados das EC, nomeadamente os auto assinados?
 - A maioria dos credenciados já vêm pré-instalados nos SO e programas (ex. Browsers)
 - Os outros podem ser adicionados pelos utilizadores: perigo!



This Connection is Untrusted

You have asked Firefox to connect securely to www.cacert.org, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

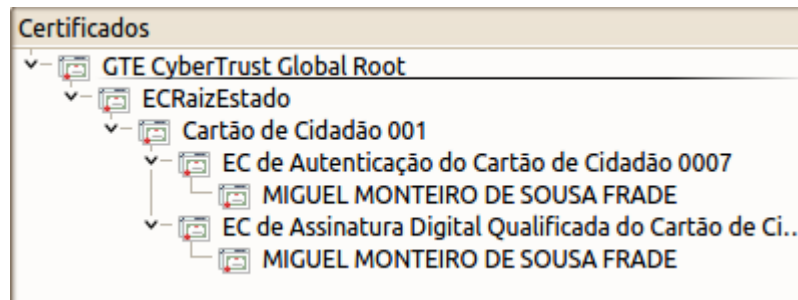
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

Como se validam assinaturas?

- Cadeia de certificados no Cartão de Cidadão



- É preciso tê-los **TODOS** para validar uma assinatura
 - O GTE já vem pré-instalado
 - Os outros são instalados com o SW do cartão
 - Ou terão de ser instalados manualmente

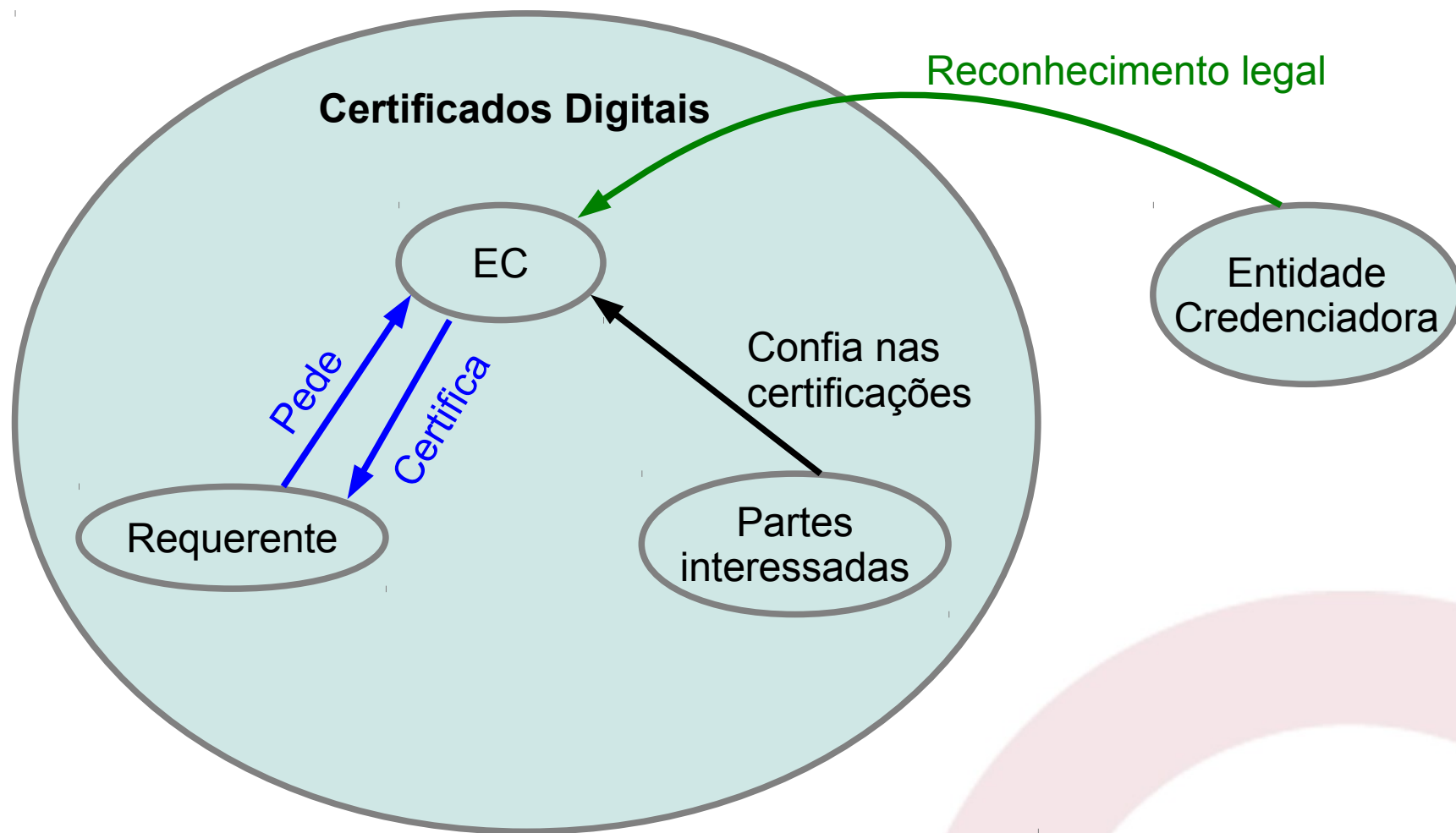
Certificados das ECs (ou certificados de raíz)

- Quem decide quais são pré-instalados?
 - Os fabricantes dos SOs e dos programas
- Posso confiar nos fabricantes?
 - Normalmente baseiam-se em listas governamentais das ECs credenciadas
 - Portugal: www.gns.gov.pt/gns/pt/tsl/
 - É preciso pagar para ser credenciado
 - » E os certificados não são gratuitos!
 - Então, isto dos certificados é um negócio?
 - Sim, também é um negócio!
 - Embora existam exceções (www.cacert.org)

Certificados das ECs (ou certificados de raíz)

- Então €€€ = segurança ?
 - Não! É preciso haver confiança no sistema.
 - Confiança
 - Não se compra
 - Não se resolve só com criptografia
 - Não se resolve só com meios técnicos
 - É preciso conquistá-la
 - » A entidade credenciadora dá credibilidade ao sistema

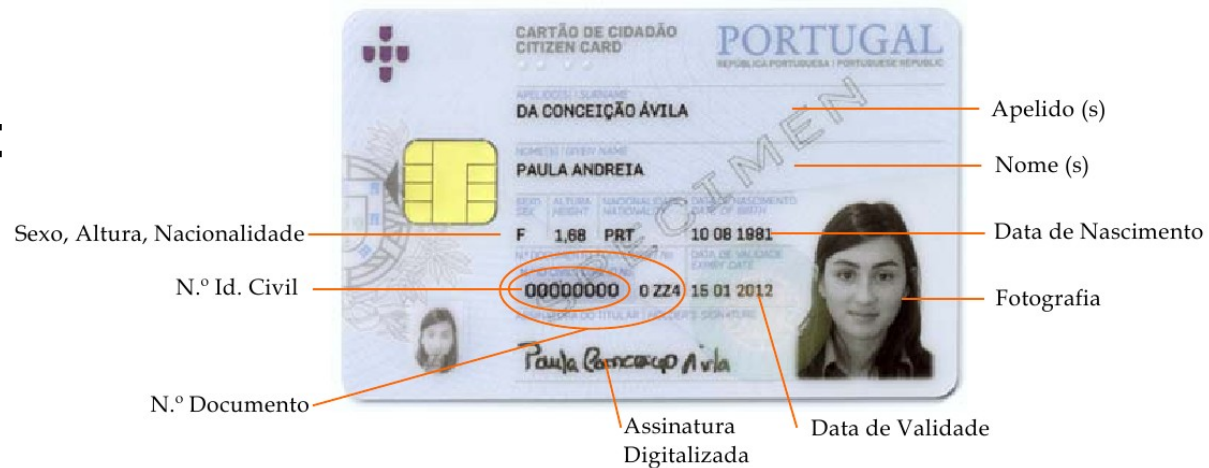
Assinaturas Digitais



Cartão de Cidadão

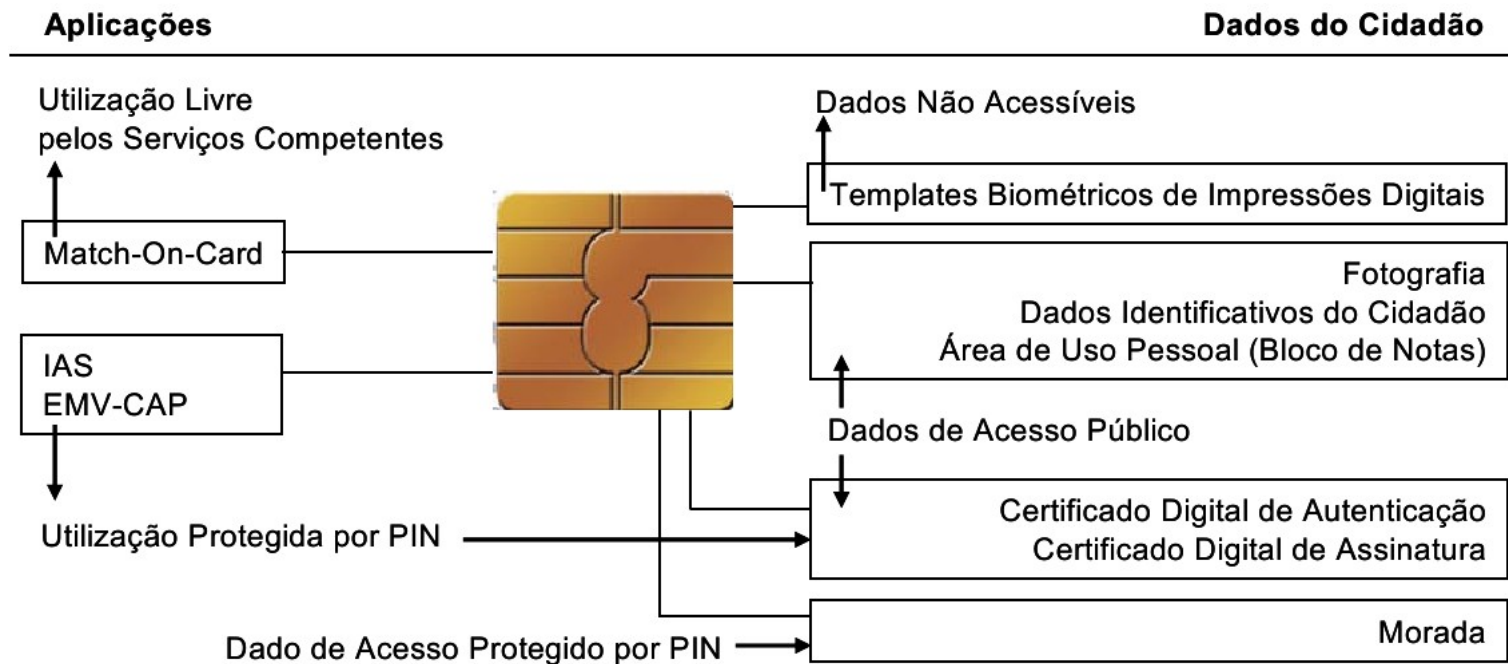
- Substitui 5 cartões:

- Bilhete de identidade
- segurança social
- cartão de contribuinte;
- cartão de utente
- cartão de eleitor (??)



Cartão de Cidadão

- Smart card (cartão inteligente): tem um microcomputador embebido




Cartão de Cidadão


- Realiza operações criptográficas
- Tem 3 PINs com 4 algarismos cada:
 - Autorizar a indicação de morada
 - Autenticação do titular
 - Produzir uma assinatura digital
 - *Assinatura electrónica qualificada certificada por entidade certificadora credenciada*


Cartão de Cidadão – Requisitos

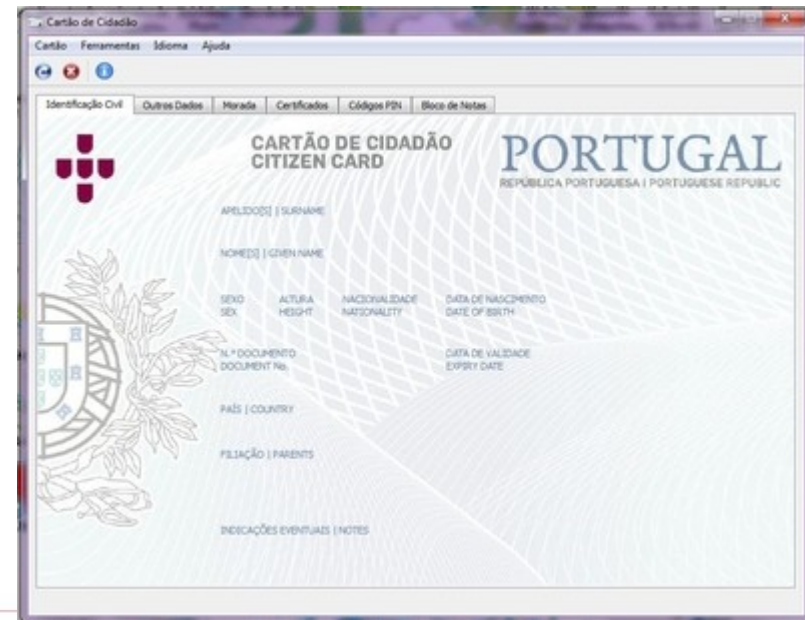
- Leitor de *smartcards*
- PINs
- Software <http://www.cartaodecidadao.pt/>



PIN da Morada: 

PIN da Autenticação: 

PIN da Assinatura Digital: 



Cartão de Cidadão

- Aplicação fornecida <http://www.cartaodecidadao.pt/>
 - Permite ver os dados visíveis no cartão físico
 - Ver a morada (com PIN)
 - Ver os certificados
 - Permite alterar os códigos PIN
 - Bloco de notas
(1000 caracteres) ????



Cartão de Cidadão

- Exercício 1 – ler os dados gravados no cartão de cidadão
 - Introduzir o cartão no leitor
 - Abrir a aplicação do “cartão de cidadão”
 - Esperar alguns segundos pela leitura
 - Navegar pelas diferentes abas

Cartão de Cidadão – Autenticação

- Alguns sítios já suportam autenticação com o CC
 - www.portaldasfinancas.gov.pt
 - <http://queixaselectronicas.mai.gov.pt>
 - <http://www.portaldasescolas.pt> (matrícula electrónica)
 - ...
- Fora do âmbito desta atividade
 - É relativamente simples de fazer
 - Consultar manual do Cartão de Cidadão

Cartão de Cidadão – Assinatura digital

- Requisitos

- Além do que já foi referenciado (PIN, leitor, SW do CC)
- Programas que permitam usar assinaturas digitais, exemplos:
 - Adobe Reader (0€) → reconhece e valida assinaturas digitais em **PDF**
 - Adobe Acrobat (700€) → reconhece, valida e faz assinaturas digitais em **PDF**
 - DigiSigner (0€ 14 dias, 35€) → reconhece, valida e faz assinaturas digitais em **PDF**
 - Thunderbird (0€), Outlook (100€) → reconhece, valida e faz assinaturas digitais nos **emails**

Cartão de Cidadão – Assinatura digital

- Exercício 2 – validar um **PDF** assinado
 - Não é preciso ter leitor de smartcards
 - Configurar o Adobe Reader:
 - 1. clique em Editar → Preferências → Assinaturas → Verificação → Integração com o Windows
 - 2. No separador Integração com o Windows e coloque um visto na 1ª opção
 - NOTA: Se o SW do CC não estiver instalado é necessário instalar TODOS os certificados primeiro
 - 3. Abrir o PDF assinado
 - Clicar em cima da assinatura

Cartão de Cidadão – Assinatura digital

- Exercício 3 – Assinar um **PDF** com o CC
 - DigiSigner → Abrir PDF a assinar
 - Assinar documento → “Não são permitidas alterações”
 - Escolher o certificado “Assinatura Digital”
 - Avançado → URL do servidor (validação cronológica):
 - <http://ts.cartaodecidadao.pt/tsa/server>
 - Algoritmo de hash: SHA256 (mais seguro)
 - Assinar

Cartão de Cidadão – Assinatura digital

- Exercício 4 – Assinar um email
 - Criar conta no Gmail só para este exercício
 - Configurar o Thunderbird e testar envio e receção de email
 - No Thunderbird:
 - Manual do cartão do cidadão: pag. 56
 - Trocar emails com os colegas
 - Validar email

Bibliografia

- Decreto de Lei nº 290/1999
- Decreto de Lei nº 62/2003
- André Zuquete, Segurança em Redes Informáticas, FCA, 4ª edição → Capítulo 3
- Manual do Software do cartão de cidadão
(https://www.portaldocidadao.pt/ccsoftware/Manual_Carta_o_de_Cidadao_v1.24.1.pdf)