Projecto Cartão de Cidadão

Especificações

Leitor Base

14 de Junho de 2007

Versão 1.0

SEMA/UMIC/AMA

ÍNDICE

1. Introdução

O presente documento tem por objectivo descrever as especificações técnicas de leitores de cartões smartcard interoperáveis com o Cartão de Cidadão.

2. Características Técnicas do Cartão de Cidadão

O Cartão de Cidadão segue as normas internacionalmente recomendadas para que este seja um documento de identificação e um documento de viagem reconhecido oficialmente. Assim, este encontra-se alinhado pelas as orientações correntes da União Europeia, nomeadamente as do grupo de trabalho para o European Citizen Card (ECC), pelas normas definidas pela International Civil Aviation Organization (ICAO) para documentos de viagem internacionais (documento 9303) e os standards 7501 e 7810 definidos pela International Organization for Standardization (ISO).

2.1. Formato e Dimensões

O formato do Cartão de Cidadão é o de um cartão ID-1, definido pela norma ISO/IEC 7810 (dimensões 85,60 × 53,98 mm) e correspondente ao formato TD-1 de machine readable travel documents (MRTD) definido pela ICAO no Documento 9303, Parte 3, Secção III. Esta norma deve ser complementada pela norma ISO 7816-2, que define a posição e funcionamento do chip embebido no cartão.

2.2. Material do Cartão

Tendo em conta em particular os aspectos de resistência física, capacidades de personalização e de incorporação de mecanismos de segurança, o Cartão de Cidadão utiliza como material de suporte o Policarbonato.

2.3. Chip

Em função dos objectivos de utilização, das aplicações previstas e das soluções neste momento perspectivadas, o *chip* do Cartão de Cidadão tem as seguintes características:

- É um *chip* Java Card, multi-aplicação;
- Suporta a versão mais recente da plataforma Java Card e o uso de *logical channels*;
- Possui uma capacidade de memória EEPROM (ou equivalente) mínima de 64 KB;
- Possui capacidades de gestão de memória dinâmica, suportando *garbage collection* pela JVM e de protecção de memória;

- Possui capacidades de gestão de espaço de armazenamento, incluindo desfragmentação e reutilização de espaço libertado;
- Possui capacidades de *true random number generation*;
- Suporta múltiplos PIN. Os PIN estão em conformidade com a norma ISO/IEC 7816-4;
- Suporta mecanismos de bloqueio em caso de erro na introdução do PIN após N tentativas e respectivo desbloqueio por meio de introdução de PUK do cidadão e de chave administrativa de acesso ao cartão, para desbloqueio;
- Suporta mecanismos de geração de novo PIN do cidadão, em caso de esquecimento deste, mediante a introdução do PUK do cidadão e de PUK aplicacional de geração de PIN;
- Possui um motor criptográfico interno que suporta:
  - Assinatura e verificação RSA de 1024 bits;
  - Assinatura electrónica qualificada segundo a norma CEN CWA 14169 (*Secure Signature-creation devices* "EAL 4+");
  - DES e TDES (*triple Data Encription Standard*);
  - MD5, SHA-1 e SHA-256, no mínimo;
  - MAC (*message authentication code*);
  - PKCS#1 (*RSA Cryptography Standard*) e PKCS#15 (*Cryptographic Token Information Format Standard*);
  - É compatível com leitores de cartões da norma EMV-CAP, para funcionamento de autenticação multicanal baseada em *one-time password*;
- Possui uma chave de protecção da personalização inicial;
- Está preparado para resistir aos ataques conhecidos do tipo "*hardware attack*", "*timing attack*", "*simple power analysis*" e "*differential power analysis*" entre outros.

3. Leitores de Cartão de Cidadão

3.1. Leitor *Desktop*

No âmbito do presente documento, são referidos como leitores *Desktop*, um modelo de leitor externo sem PIN-pad nem lógica aplicacional, para ligação a um computador pessoal e comunicação com aplicações existentes no Cartão de Cidadão. A *interface* com o cartão é de contacto.

3.2. Especificações Técnicas

3.2.1. Requisitos base

3.2.1.1. Interfaces

3.2.1.1.1. Físicos

O *interface* físico dos leitores "conectáveis" (i.e. Leitores *Desktop* e Leitores *All-in-One*) com computadores pessoais, deverá ser USB (1.1 ou 2.0).

3.2.1.1.2. Lógicos

Os leitores deverão estar de acordo com as normas:

- PC/SC versão 1.0;
- ISO/IEC 7816-1,2,3,4: *IC Cards with Contacts*;
- EMV Level 1;
- CT-API versão 1.1;
- CCID – Chip Card Interface Device 1.0;

3.2.1.1.3. Smartcard

O *interface* do leitor com o Cartão de Cidadão deverá:

- Suportar a norma ISO/IEC 7186 Class A, B e C (*smarcards* com voltagens de 5V, 3V, 1.8V);

- Suportar leitura e escrita para smarcards com microprocessadores alinhados com ISO/IEC 7816-1,2,3,4, protocolos T=0 e T=1;
- Suportar *smartcards* com frequências de relógio até 8Mhz;

3.2.1.2. Drivers (Sistemas Operativos)

Os *drivers* PC/SC dos leitores (excepto leitor OTP – *One-Time Password*, e leitores com suporte para cidadãos com deficiências visuais) deverão suportar os seguintes sistemas operativos:

- Windows XP;
- Windows 2000;
- Windows Server 2003;
- Windows ME;

O leitor deverá ainda possuir *drivers* para utilização em Linux e Mac OS X.

3.2.1.3. Certificações

Os leitores deverão ainda ter as seguintes certificações:

- Microsoft Windows Hardware Quality Labs (WHQL) – caso o sistema operativo seja Windows;
- Microsoft Windows Logo Program WLP 2.0 – caso o sistema operativo seja Windows;
- EMV Level 1 (EMV2000);

3.2.1.4. Formato dos Cartões

Os leitores deverão suportar *smartcards* de formato ID-1.

3.2.1.5. Normas CE

Os leitores deverão ainda estar de acordo com as normas em vigor da Comunidade Europeia relativas à segurança de produtos (selo CE), e redução de substâncias perigosas (RoHS).

3.2.1.6. Voltagens suportadas

Os leitores deverão suportar *smartcards* com voltagens de 1.8V, 3V e 5V.