Ministério da Justiça

Termo de Cooperação/Projeto:

Acordo de Cooperação Técnica FUB/CDT e MJ/SE Registro de Identidade Civil – Replanejamento e Novo Projeto Piloto

Documento:

RT Diagnóstico de eID e pesquisa de tecnologias

Parte II: Levantamento de tecnologias referentes a eID´s

Data de Emissão:

31/07/2015

Elaborado por:

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB

MINISTÉRIO DA JUSTIÇA

José Eduardo Cardozo
Ministro

Marivaldo de Castro Pereira
Secretário Executivo

Hélvio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

UNIVERSIDADE DE BRASÍLIA

Ivan Marques Toledo Camargo
Reitor

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA

Ana Maria da Consolação Gomes Lindgren
Andréa Benoliel de Lima
Celso Pereira Salgado
Delluiz Simões de Brito
Elaine Fabiano Tocantins
Fernando Saliba Oliveira
Fernando Teodoro Filho
Guilherme Braz Carneiro
Joaquim de Oliveira Machado
José Alberto Sousa Torres
Marcelo Martins Villar
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

EQUIPE TÉCNICA

Flávio Elias Gomes de Deus (Pesquisador Sênior)
William Ferreira Giozza (Pesquisador Sênior)
Ademir Agustinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alysson Fernandes de Chantal
Andréia Campos Santana
Antônio Claudio Pimenta Ribeiro
Carolinne Januária de Souza Martins
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Diogenes Ferreira Reis Fustinoni
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Glaidson Menegazzo Verzeletti
Heverson Soares de Brito
Johnatan Santos de Oliveira
José Carneiro da Cunha Oliveira Neto
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Antônio de Souto Evaristo
Luiz Claudio Ferreira
Marco Schaffer
Marcos Vinicius Vieira da Silva
Pedro Augusto Oliveira de Paula
Roberto Mariano de Oliveira Soares
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Suzane Lais De Freitas
Valério Aymoré Martins
Vera Lopes de Assis
Wladimir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autores
31/06/2015	0.1	Versão inicial do RT Diagnóstico sobre eID´s e pesquisa de tecnologias - Levantamento de tecnologias referentes a eID´s.	Sandro Haddad
31/07/2015	0.2	Versão para homologação, conforme recomendações e considerações finais solicitadas pelo MJ	Sandro Haddad

latitude
Laboratório de tecnologias da tomada de decisão

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

SUMÁRIO

1 GLOSSÁRIO

AES - Advanced Encryption Standard

CC - Common Criteria

DDA - Dynamic data authentication.

DES - Data Encryption Standard.

ECC - Elliptic Curve Cryptography

EMV - Europay MasterCard Visa.

EPROM - Erasable programmable read-only memory.

EEPROM - Electrically erasable programmable read-only memory.

EAL - Evaluation assurance level

FIPS - Federal Information Processing Standard

FRAM - Ferroelectric random access memory

FLASH memory - A type of EEPROM

IC - Integrated Circuits

IEC - International Electrotechnical Commission.

ISO - International Organization for Standardization

MCU - Microcontroller Unity

NFC – Near Field Communication

NIST - National Institute of Standards and Technology.

PIN - Personal identification number.

PP - Protection profile

RAM - Random access memory.

ROM - Read-only memory

SDA - Static data authentication.

2 INTRODUÇÃO

A Secretaria Executiva (SE/MJ), vinculada ao Ministério da Justiça (MJ), é responsável por viabilizar o desenvolvimento e a implantação do Registro de Identidade Civil, instituído pela Lei nº 9.454, de 7 de abril de 1997, regulamentado pelo Decreto nº 7.166, de 5 de maio de 2010.

Atualmente, a República Federativa do Brasil conta com sistema de identificação de seus cidadãos amparado pela Lei nº 7.116, de 29 de agosto de 1983. Essa lei assegura validade nacional às Carteiras de Identidade, ou Cédulas de Identidade; confere também autonomia gerencial às Unidades Federativas no que concerne à expedição e controle dos números de registros gerais emitidos para cada documento. Essa condição de autonomia, ao contrário do que pode parecer, fragiliza o sistema de identificação, já que dá condições ao cidadão de requerer legalmente até 27 (vinte e sete) cédulas de identidades diferentes. Com essa facilidade legal, inúmeras possibilidades fraudulentas se apresentam de maneira silenciosa, pois, na grande maioria dos casos, os Institutos de Identificação das Unidades Federativas não dispõem de protocolos e aparato tecnológico para identificar as duplicações de registro vindas de outros estados, ou até mesmo do seu próprio arquivo datiloscópico. Consoante aos fatos, os Institutos de Identificação não trabalham interativamente para que haja trocas de informações de dados e geração de conhecimento para manuseio inteligente e seguro para individualização do cidadão em prol da sociedade.

Com foco na busca de soluções para tais problemas, o Projeto RIC prevê a administração central dos dados biográficos e biométricos dos cidadãos no Cadastro Nacional de Registro de Identificação Civil (CANRIC) e ABIS (do inglês *Automated Biometric Identification System*), respectivamente. A previsão desse novo modelo sustenta a não duplicação de registros e a consequente identificação unívoca dos cidadãos brasileiros natos e naturalizados. O Projeto RIC, portanto, visa otimizar o sistema de identificação e individualização do cidadão brasileiro nato e naturalizado com vistas a um perfeito funcionamento da gestão de dados da sociedade, os quais agregam valor à cidadania, à gestão administrativa, à simplificação do acesso aos serviços disponíveis ao cidadão e à segurança pública do país.

Nesse contexto, o termo de cooperação entre MJ/SE e FUB/CDT define um projeto que objetiva identificar, mapear e desenvolver parte dos processos e da infraestrutura

tecnológica necessária para viabilizar a implantação do número único de Registro de Identidade Civil – RIC no Brasil.

O presente documento tem como objetivo geral apresentar uma revisão teórica das características e especificações elétricas do *Chips* implementados nos sistemas eletrônicos de eID (*electronic Identity*) *cards*.

3 Estudo das normas técnicas referentes a *chips* com contato e sem contato

O propósito geral do uso de Circuitos Integrados, ou também denominados *Chips*, em *Smart Cards* e em eID *cards*, é o armazenamento seguro de informações pessoais específicas que permitam uma identificação correta da identidade de uma pessoa.

Do ponto de vista do *chip*, estas informações pessoais específicas são tratadas basicamente como sendo dados que devem ser armazenados com segurança. Ou seja, que sejam preservadas a confidencialidade e a integridade dos dados e que os mesmos sejam acessados por meio de mecanismos seguros, com proteção adequada da privacidade, utilizando algoritmos de criptografia [1].

O potencial de aplicações de um *smart card* é extremamente variável. Com o crescente aumento da capacidade de processamento e no tamanho das memórias disponíveis nos Circuitos Integrados (CI´s) atuais, a faixa de aplicações continua se expandindo. Na Fig.1, são apresentadas as capacidades de memórias e de processamento para algumas aplicações dos *smart cards*.

Os algoritmos de criptografia implementados nos *chips* de eID *cards* cobrem uma grande variedade de técnicas, vão desde primitivas bastante conhecidas, como por exemplo, o DES e o AES, bem como protocolos de autenticação eletrônica, como o PACE e o EAC. A definição destes algoritmos e protocolos de criptografia é fornecida pelas autoridades de cada país, por meio de relatórios técnicos dos cartões de eID ou por meio de padrões técnicos [1].

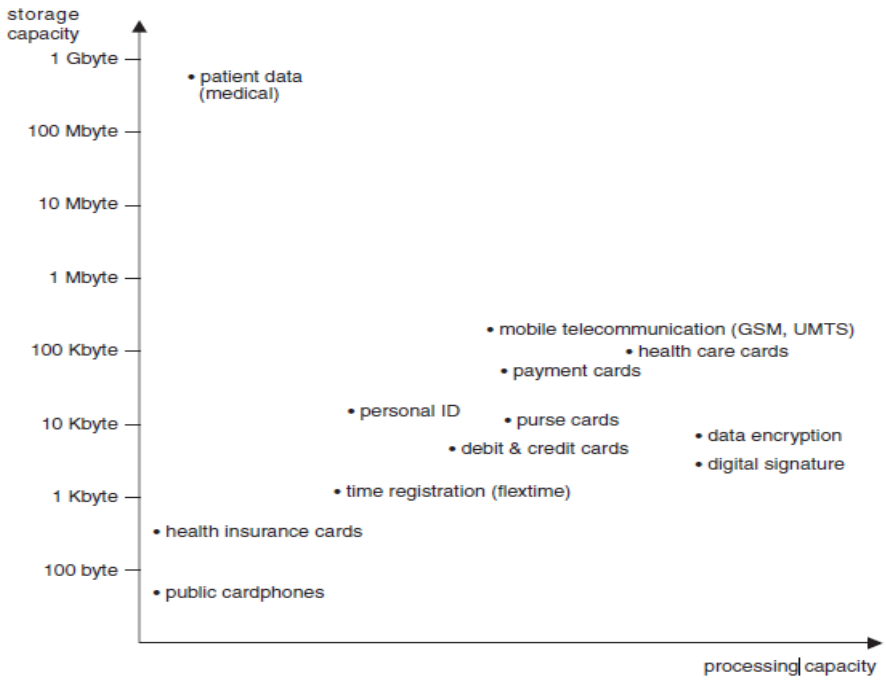


Fig. 1 - Aplicações de *smart cards*, com as respectivas capacidades de armazenamento e processamento. Fonte: [2]

3.1 *Chips* eID

Os *chips* com microprocessadores empregados em *smart card* e eID apresentam alguns componentes fundamentais, apresentados na Fig.2. Uma análise de projetos lançados e produtos de mercado, mostra que os microprocessadores utilizados em *Smartcards* são específicos para estas aplicações, ou seja, não são utilizados os processadores "padrões" largamente utilizados pela indústria eletrônica de consumo. Os motivos desta especificidade do microprocessador são: custo de fabricação, funcionalidade (coprocessador criptográfico), segurança contra ataques, aplicação multi-tarefa e limitação da área do silício (imposto pelo cartão de aproximadamente 25mm^2) [2].

- Interface de comunicação para o leitor externo

  - Estas interfaces seriais de dados podem ser definidas como: com-contato *(Contact)* definidas pela norma ISO/IEC 7816-3, *ou sem-contato (Contactless)*, definidas pela norma ISO/IEC 14443, ambas controladas pela CPU. Alguns modelos recentes de *chips* integram também uma interface USB com taxa de transferência

de até 480 Mbps [2], e a interface ISO/IEC 14443 com a taxa muito alta (VHBR) de até 6.8Mbps, que já é usada na nova eID da Espanha.

- CPU (Unidade de processamento central)

  - Controla as funções básicas de todo o *chip* e da memória não-volátil;

- Memória não-volátil

  - Normalmente implementada com EEPROM (*Electrically Erasable Programmable Read Only Memory* - Memória somente de leitura programável eletricamente apagável) ou *Flash*;

  - Esta memória é utilizada para o armazenamento seguro de informações importantes, como por exemplo, chaves de criptografia (*encryption keys*) e certificados de segurança;

  - A célula da EEPROM é essencialmente um transistor MOS (capacitor fino). No entanto, para carregar a célula, é necessário uma tensão elevada (dezenas de Volts), assim, um circuito *Charge-pump* é implementado, aumentando a área e a complexidade desta memória.

  - A memória *Flash* apresenta um tempo de acesso bem menor (micro segundos) do que a memória EEPROM (milissegundos). Além disso, dependendo da estrutura, a célula *Flash* pode ser até 4 vezes menor que a EEPROM (próximo do tamanho da ROM, podendo substituí-la). A desvantagem é que as memórias *Flash* possuem menor número médio de ciclos de leitura/escrita (10^5 vezes), comparado à EEPROM (10^6 vezes) [2].

  - A célula da *Flash* apresenta uma funcionalidade e estrutura do transistor MOS similar à EEPROM. No entanto, o princípio de escrita da *Flash* é baseado no efeito de injeção de elétrons, reduzindo assim o tempo de escrita, e a EEPROM no efeito de tunelamento.

  - Existem dois tipos de células *flash*: NOR e NAND. Devido às diferentes conexões internas, as células *Flash* NOR são utilizadas para armazenar códigos de programa e as NAND para armazenar dados.

  - Devido a limitações tecnológicas, é difícil fabricar memória EEPROM e *Flash* em uma mesma pastilha de silício (*chip*).

- As memórias EPROM só podem ser apagadas com exposição a luz UV. Ou seja, não podem ser apagadas em um *smart card* e, portanto, EPROM não são utilizadas.

- A memória FRAM (RAM Ferroelétricas) não são voláteis como a RAM, mas apresentam um tempo de escrita equivalente à RAM. No entanto, os materiais e etapas de processo de fabricação da memória FRAM não são comumente utilizados na indústria de semicondutores.

- Memória RAM

- Memória RAM (*Random Acess Memory*) é uma memória volátil, que mantém os dados somente quando aplicada uma tensão de alimentação (VDD ou Vcc) no *chip*;

- Utilizada pelo controlador como uma memória operacional, que armazena variáveis, resultados intermediários da CPU e dados de entrada/saída (*input/output buffer*);

- *As vantagens da memória RAM são a rápida velocidade de leitura e escrita, em torno alguns de nanosegundos. A topologia mais utilizada é a SRAM (Static RAM). No entanto, uma célula de memória RAM ocupa uma grande área.* De uma forma geral, a memória RAM ocupa, para uma mesma memória, aproximadamente 4 vezes mais área do que uma célula de memória EEPROM, que por sua vez, ocupa 4 vezes mais área que uma célula ROM [2]. Este é o principal motivo pelo qual os microprocessadores apresentam memórias RAM pequenas.

- Memória ROM

- A memória ROM (*Ready Only Memory*) armazena o *software* do Sistema Operacional, por meio de instruções binárias na CPU, e funções da memória não volátil EEPROM/*Flash*. As informações da memória ROM são permanentemente armazenadas no momento em que o *chip* é fabricado.

- Co-processador de criptografia

- O co-processador de criptografia implementa em hardware diversas operações criptográficas, permitindo uma alta eficiência nos cálculos matemáticos, necessários para as funções de criptografia.

- Os co-processadores geralmente implementam os algoritmos de criptografia simétricos, como o DES e o AES, e os assimétricos, como o RSA e curvas-elípticas.

- Gerador de Números Aleatórios (RNG -*Random Number Generator*)

- Um requisito de segurança chave de todos os sistemas que implementam protocolos criptográficos, como geração de chaves de sessão, é a disponibilidade de números aleatórios fornecidos por um circuito denominado RNG, implementado em *Hardware*.

- Por razões de segurança, os *smart cards* devem apresentar um gerador de números aleatórios genuínos (implementado em *Hardware*), ao invés de um gerador pseudoaleatório (comumente implementado por *Software*).

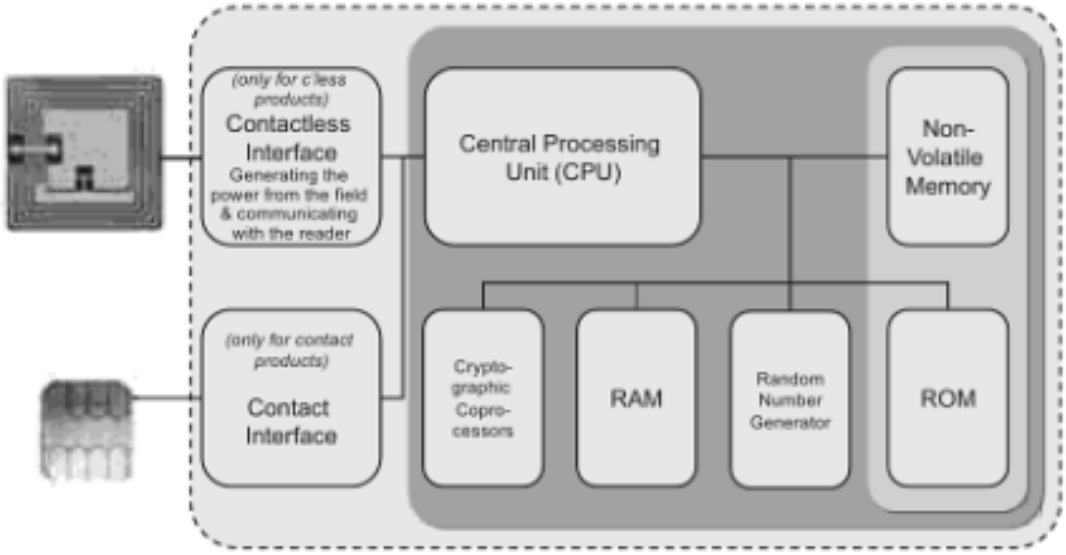
- Geralmente os RNGs devem atender os requisitos do padrão FIPS140-2.

- Unidade de Gerenciamento de Memória (MMU- *Memory Management Unit*)

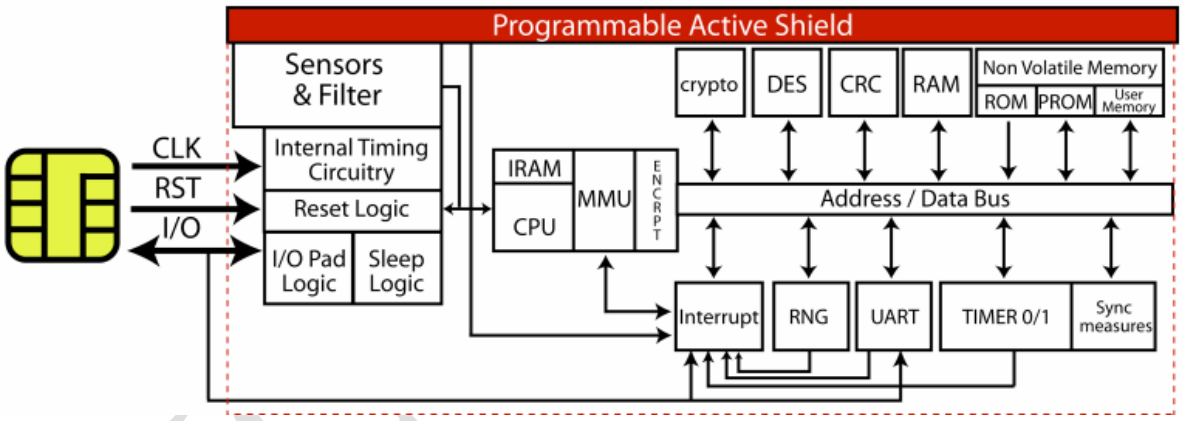
- Os sistemas operacionais dos *Smartcards* modernos multipalicação permitem a execução de diversas aplicações, cujos códigos são gravados em uma mesma memória.

- Afim de evitar que o código de uma aplicação, denominado *applet*, tenha acesso a dados secretos de uma outra aplicação, é implementada uma Unidade de Gerenciamento de Memória (MMU) no *chip*. A MMU permite que apenas uma parte determinada da memória seja acessada pelo código de cada *applet*.

- No momento, apenas alguns microprocessadores para *Smartcards* apresentam uma unidade MMU. Além disso, o tipo de MMU implementado tem um grande impacto no desenvolvimento dos sistemas operacionais, limitando assim, a portabilidade destes programas, pois o acesso das memórias e as definições de endereçamento variam de acordo com as funções de proteção encontradas na MMU.



(a)



(b)

Fig. 2 - Blocos funcionais de um *chip* de eID (a) [1], e componentes de segurança como sensores e MMU (b) [15]

Vale ressaltar que todos estes elementos descritos anteriormente são implementados utilizando somente um circuito integrado, ou seja, são monoliticamente integrados em uma única pastilha de silício. Uma configuração típica dos *chips* eID atuais está descrita na Tabela 1.

Tab. 1 - Configuração e características de um *chip* eID estado-da-arte [1]

Memórias e Coprocessador criptográfico	*Chips* eID típicos
Memória não-volátil [Kbyte]	18-144
RAM [Kbyte]	6
ROM [Kbyte]	300-400
Coprocessador criptográfico	3DES, RSA, AES

Na Tabela 2 é descrita uma porcentagem típica utilizada pelos componentes na área total do microprocessador de um *smart card*.

Tab. 2 - Distribuição (em % da área total) dos componentes do microprocessador [2]

Componente	Área
CPU	20%
RAM	15%
ROM	10%
EEPROM	45%
Outros	10%

3.2 *Chip* eID "com-contato" (*Contact*)

Circuitos Integrados (CI´s) ou *chips* "com-contato" (*Contact Chips*) para *smart cards* suportam uma interface padronizada de acordo com ISO/IEC 7816, como demonstrado na Fig. 3.

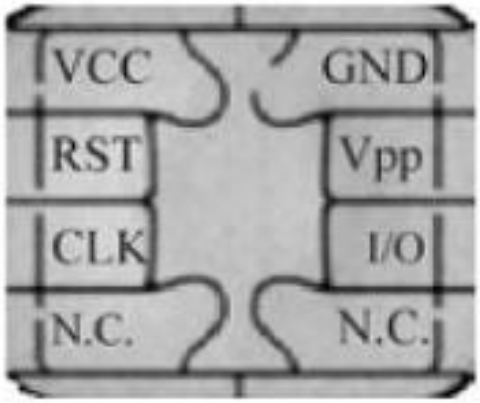


Fig. 3 - Módulo de contato ISO 7816

O módulo de contato consiste em uma conexão de 6 ou 8 pinos:

- Tensão de alimentação (*Supply voltage*) - VDD ou VCC;
  - Vcc = 5V - Classe A (definida pela ISO 7816)
  - Vcc = 3V - Classe B
  - Vcc = 1.8V - Classe C
- Terra (*Ground*) - GND;
- Pino de *Reset* - RST;
- Entrada do *Clock* de frequência - CLK;
  - Alguns CI´s possuem *clocks* internos;
  - De acordo com o padrão ISO, a máxima taxa externa do *clock* é 10MHz (não é limitada pela performance da CPU);
- Entrada/Saída serial de dados (*Input/Output*) - I/O;
  - A frequência do *clock* de 10MHz limita a taxa de transmissão da interface I/O serial em 312 Kbits/s [1].
- Tensão de programação da EEPROM- Vpp: Na prática, como a tensão pode ser normalmente gerada internamente no *chip* por meio de um circuito *charge pump*, o contato fica disponível para outros usos como pela interface USB.
- Pinos não conectados (reservado para aplicações futuras) - N.C.

3.3 *Chip* eID "sem-contato" (*Contactless*)

A operação dos *Smartcards* "sem-contatos" (*Contactless*) é baseada em um acoplamento indutivo entre o leitor e o *chip*, através de um campo magnético gerado pela bobina (*coil*) do leitor e recebido por uma outra bobina no cartão, denominada de antena.

O *link* indutivo é utilizado para fornecer energia para o *chip* do cartão e para transmitir dados em ambas direções, conforme mostrado na Fig.4. A frequência de transmissão normalmente é de 13.56 MHz.

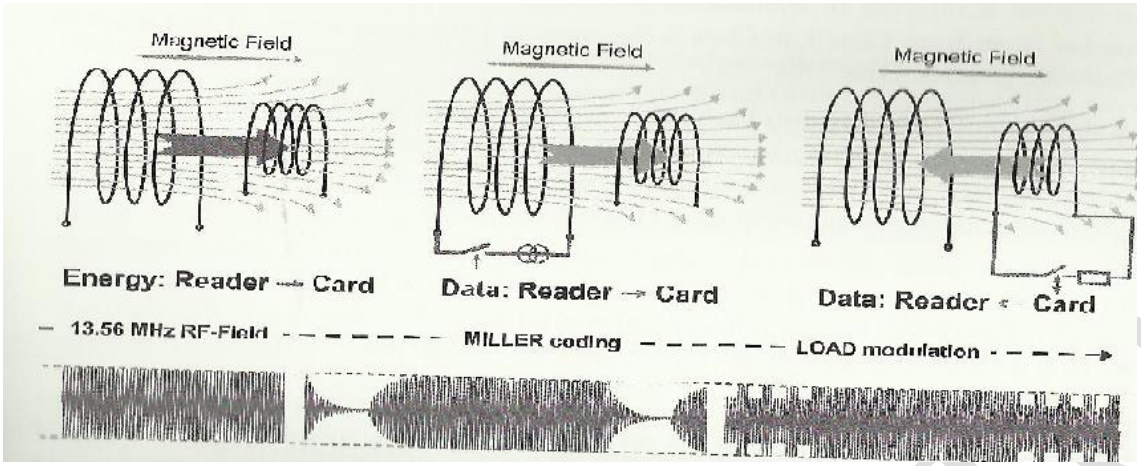


Fig.4 - Transmissão de dados do *chip* "sem-contato" [1]

- *Down-link* (leitor-cartão): Modulação FSK (*Frequency Shift Keying*) ou (seria "com".) *Miller coding*;
- *Up-link* (cartão-leitor): Modulação ASK (*Amplitude Shift Keying*);

Para que seja estabelecida um *link* de comunicação robusto, alguns critérios do sistema devem ser otimizados:

- Os circuitos analógicos e digitais do CI devem ser projetados utilizado técnicas de ultra baixo consumo de potência *(ultra low-power*) devido à energia limitada fornecida pelo campo magnético;
- A implementação do sistema deve estar de acordo com padrões internacionais [ISO14443]. O sistema leitor-cartão deve garantir a interoperabilidade (*interoperability*) através de uma implementação eficiente e uma otimização de performance, completamente de acordo com os padrões.
- Os parâmetros da antena devem ser definidos para uma faixa larga de frequência.
- A distância entre o leitor e o cartão determina a energia fornecida para o dispositivo. O dispositivo (cartão) deve apresentar uma performance otimizada com relação ao seu consumo de potência, apresentando um gerenciamento adaptativo de seu consumo de potência;
- A performance do cartão "sem-contato" depende do tamanho da antena. Quanto maior a antena, maior será o fluxo magnético e assim, maior será a corrente de polarização disponível para o *chip*. Os parâmetros de tamanho para algumas

classes de antenas nos cartões estão disponíveis na Tab. 2.

Tab.2 - Parâmetros e classes das antenas dos cartões "sem-contato"

	Classe 1	Classe 2	Classe 3	Classe 4	Classe 5	Classe 6
Área externa (mm)	87 x 49	81 x 27	50 x 40	50 x 27	40,5 x 24,5	25 x 20
Área interna (mm)	64 x 34	51 x 13	35 x 24	35 x 13	25 x 10	-

3.4 Sensores e *Hardware* de segurança

Os Circuitos Integrados (CI´s) são projetados para funcionarem com determinados valores de tensão de alimentação, frequência e temperatura. Normalmente, nas especificações elétricas destes circuitos são definidas faixas de variação dos valores típicos, nas quais o funcionamento do circuito seja garantido. Além das faixas de variações pré-definidas, existe uma área onde os circuitos integrados deixam de funcionar corretamente. Acima destas áreas de mau funcionamento, os circuitos deixam de funcionar.

Para CI´s de alta segurança como os *chips* para eID, é necessário evitar que os circuitos operem nestas faixas de mau funcionamento, evitando assim um ataque externo forçado que gere um comportamento inadequado, como por exemplo, falhas na validação dos algoritmos de segurança, ou interrupção de execução que permita a leitura de valores de registradores.

Atualmente os CI´s aplicados em sistemas de segurança apresentam sensores que irão reiniciar o *chip* sempre que os circuitos forem forçados a operar em limites acima dos valores pré-estabelecidos. Ou seja, os CI´s possuem tensões de referências internas, *bandgaps*, e osciladores internos, gerando *clocks* de referência, que medem e comparam os valores externos aplicados para a temperatura, tensão de alimentação e a frequência do *clock*, e tomem a decisão de aplicar um *reset* no *chip* sempre que os limites definidos forem

ultrapassados, conforme mostrado na Fig. 5.

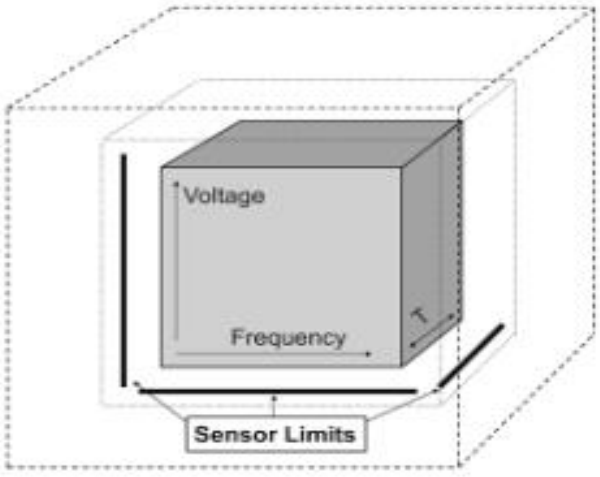


Fig. 5 - Limites de valores aplicados de frequência, temperatura e tensão para CI´s de segurança [1]

3.5 Norma ISO/IEC 14443 - Cartões com CI´s Sem-Contato (*Contactless*) (2a edição - 2008)

As normas dos cartões Sem-Contato (SC, ou em inglês, *Contactless*) abrangem uma variedade de tipos de cartões descritos nas seguintes normas: ISO/IEC 10536 (*close-coupled cards* - cartões de acoplamento fechado), ISO/IEC 14443 (*proximity cards* - cartões de proximidade) e ISO/IEC 15693 (*vicinity cards* - cartões de arredores). Esses tipos de dispositivos são destinados, respectivamente, para a operação inserido no leitor, muito próximo, e a uma longa distância, a partir de dispositivos de acoplamento e leitura associados.

A norma ISO/IEC 14443 define os requisitos específicos de tecnologia para cartões de identificação em conformidade com as normas ISO/IEC 7810 e ISO/IEC 15457-1. Além disso, a ISO/IEC 14443 detalha a operação de cartões de proximidade na presença de outros cartões sem contacto, em conformidade com a ISO/IEC 10536 e ISO/IEC 15693.

A segunda edição desta norma internacional (2008) cancelou e substituiu a primeira edição ISO/IEC 14443-1:2000, a qual foi revisada tecnicamente. A norma ISO/IEC 14443 consiste em quatro partes:

- Parte 1: Características físicas;
- Parte 2: Potência de RF (Rádio Frequência) e interferência do sinal;
- Parte3: Inicialização e anticolisão;
- Parte 4: Protocolo de transmissão.

Uma breve descrição de algumas partes desta norma, com as principais características técnicas, será apresenta nas subseções seguintes.

3.5.1 Características físicas (Parte I) - ISO/IEC 14443-1

O PICC (*Proximity Integrated Circuit Cards* - Cartão de proximidade com Circuito Integrado) poderá ter as dimensões definidas pela ISO/IEC 7810 ou ISO/IEC 15457-1. Porém, caso as dimensões não atendam às normas, as dimensões da antena não poderão exceder 86 mm × 54 mm × 3 mm. Esta restrição se deve pelo fato de que a Potência de RF e interferência de sinal definidos pela ISO/IEC 14443-2 e a metodologia de testes definida pela ISO/IEC 10373-6. A posição e dimensionamento interno e externo estão apresentados na Fig. 6.

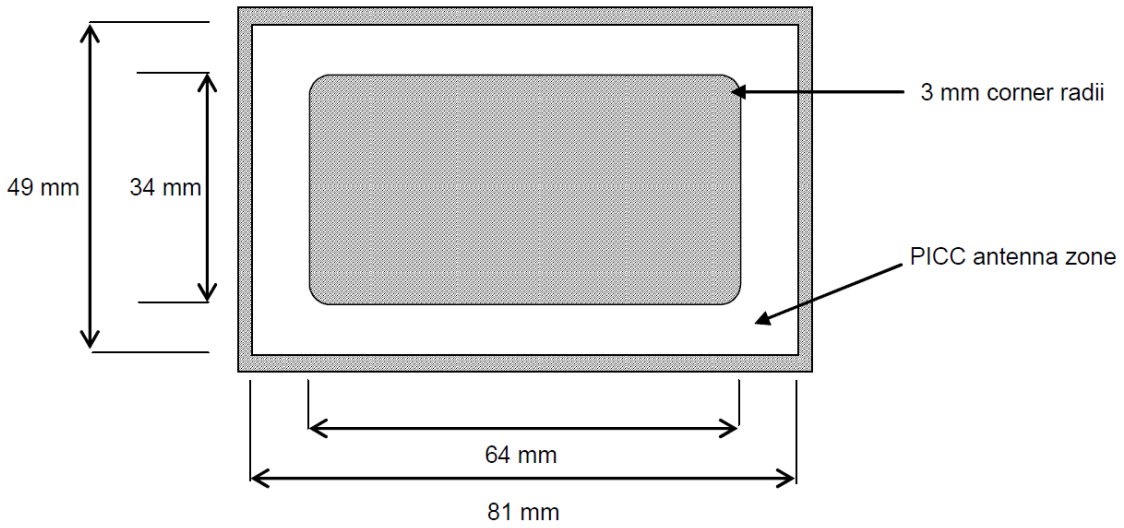


Fig.6 - Dimensões físicas dos cartões PICC

O uso de classes do PICC é opcional. Caso seja utilizado, deve atender aos requisitos no anexo A. No setor industrial, a definição de classes auxilia na interoperabilidade.

O nível médio do campo magnético aplicado continuamente no cartão deverá ser de 10 A/m RMS na frequência de 13,56 MHz, com um tempo médio de exposição de 30 segundos. O nível máximo deste campo magnético é limitando a 12 A/m RMS.

3.5.2 Protocolo de Transmissão (ISO/IEC 14443-4)

A segunda edição desta norma internacional (2008) cancelou e substituiu a primeira edição ISO/IEC 14443-4:2001 e incorpora os adendos da ISO/IEC 14443-4:2001/Amd.2006.

A parte IV especifica o protocolo de transmissão do bloco *half-duplex*. As unidades de dados do protocolo de aplicação poderão ser mapeadas pela norma ISO/IEC 7816-4. O escopo desta norma ISO/IEC 14443-4 define a sequência de ativação e desativação do protocolo aplicados em cartões de proximidade ou objetos do Tipo A e Tipo B.

Uma das vulnerabilidades do uso de interface ISO/IEC 14443 é a possibilidade de rastreamento do chip, e medidas de proteção específicas devem ser adotadas no projeto da eID.

3.6 Norma ISO/IEC 7816 - Cartões com CI´s Com-Contato (*Contact*)

A norma ISO/IEC7816 além de especificar a interface com contato, define especificações como referentes ao intercâmbio de dados e comandos C-APDU, e é também usada na especificação de chips com interface sem contato. A norma IS0/IEC 7816 consiste nas seguintes partes:

- Parte 1: Características físicas;
- Parte2: Dimensões e localização dos contatos;
- Parte 3: Sinais Eletrônicos e protocolos de transmissão;
- Parte 4: Comandos Interindustriais (*Interindustry*) para intercâmbio (*Interchange*);
- Parte 5: Sistema de numeração e procedimentos de registro para identificador de aplicação;
- Parte 6: Elementos de dados de interindustrial (*Interindustry*);
- Parte 7: Comandos interindustrial para linguagem *query* de cartões estruturados;

- Parte 8: Comandos interindustrial relacionados à segurança;
- Parte 10: Sinais eletrônicos e resposta para o *reset* para cartões síncronos;
- Parte 11: *Personal verification through biometric methods;*
- Parte 12: *Cards with contacts* — USB *electrical interface and operating procedures;*
- Parte 13: *Commands for application management in multi-application environment*
- Parte 15: *Cryptographic information application.*

A seguir serão descritas algumas partes da norma ISO/IEC 7816.

3.6.1 Características físicas (Parte I) - ISO/IEC 7816-1:1998

Este padrão foi revisado e atualizado pelo ISO/IEC 7816-1:2011, além da norma complementar Adendo 1:2003 - Máxima altura da superfície de contato do CI, que especifica que nenhum ponto de toda superfície de contato do CI pode estar acima de 0.10mm ou abaixo de 0.10mm da superfície do cartão.

As características físicas descritas a seguir definem o cartão depois da inclusão de CI´s com contatos em um cartão tipo ID-1. O cartão com CI também deve atender aos requisitos das normas ISO/IEC 7811-1 a ISO/IEC 7811-6 e ISO/IEC 7813.

- *Luz Ultra-violeta:* Qualquer proteção para luz ultravioleta deve ser de responsabilidade do fabricante do cartão.
- *Raios-X:* Uma exposição de 0,1 Gy de uma energia média de radiação de 70keV até 140 keV (por ano) não deve causar mal funcionamento do cartão.
- *Estresse mecânico (cartão e contatos):* Cada superfície de contato e a área de contato (toda a superfície galvânica) não poderá sofrer danos sobre uma pressão de trabalho equivalente a uma esfera de aço de 1mm de diâmetro aplicando uma força de 1,5N.
- *Resistência elétrica dos contatos:* Quando aplicada uma corrente DC com valor entre 50uA e 300mA, a resistência entre dois contatos deve ser menor que 0,5Ω. A impedância deve ser definida como sendo: um valor de tensão sobre esta impedância menor que 10mV para uma corrente AC de pico de 10mA na frequência de 4MHz (Z= 1 V/A @ 4MHz).

- *Interferência Eletromagnética (entre a tarja magnética e o CI):* Caso o cartão tenha uma tarja magnética, o CI do cartão não deve sofrer danos quando os dados da tarja magnética forem lidos, escritos ou apagados. Analogicamente, a escrita e leitura do CI também não deve causar danos na tarja magnética.
- *Eletricidade Estática:* A performance do cartão não poderá ser degradada devido à uma descarga estática, de um capacitor de 100pF, entre o contato e o terra (*ground*) com uma tensão de 2000V através de uma resistência de 1500Ω (uso normal por uma pessoa com carga eletroestática).
- *Temperatura de operação:* O CI deve funcionar entre 0 ºC e 50 ºC.
- *Propriedades de flexão:* Quando submetido à 1000 ciclos de flexão, conforme descrito na ISO/IEC 10373:1993, o cartão deverá continuar funcionando e não poderá apresentar partes quebradas.
- *Propriedade de Torção:* Quando submetido à 1000 ciclos de torção, conforme descrito na ISO/IEC 10373:1993, o cartão deverá continuar funcionando e não poderá apresentar partes quebradas.

3.6.2 Dimensão e localização dos contatos (Parte II) - ISO/IEC 7816-2:2007

A segunda edição desta norma internacional (ISO/IEC 7816-2:2007) cancelou e substituiu a primeira edição ISO/IEC 7816-2:1999 e incorpora os adendos da ISO/IEC 7816-2:1999/Amd.1:2004.

Dimensões mínimas do contato

A norma define que o contato deve ter uma superfície retangular mínima de 2mm x 1,7mm, conforme apresentado na Fig.7. A norma não define as dimensões máximas nem o formato do contato.

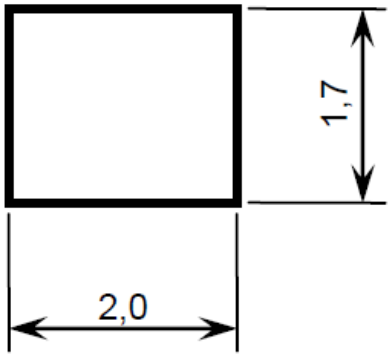
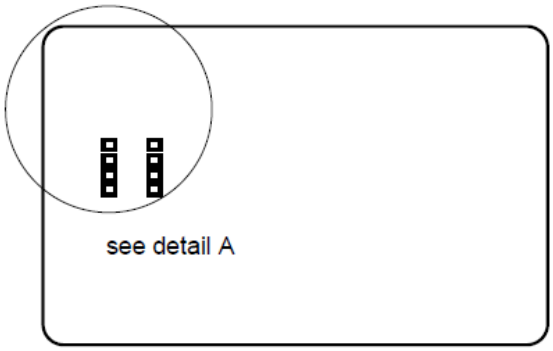


Fig.7 - Mínimas dimensões do contato *(em milímetros)*

Localização dos contatos

Esta parte da norma define 8 contatos, C1 -C8. Os contatos deverão estar localizados na frente do cartão e deve ser localizado de acordo com a Fig.8. Cada contato deve ser definido de acordo com a ISO/IEC 7816-3.



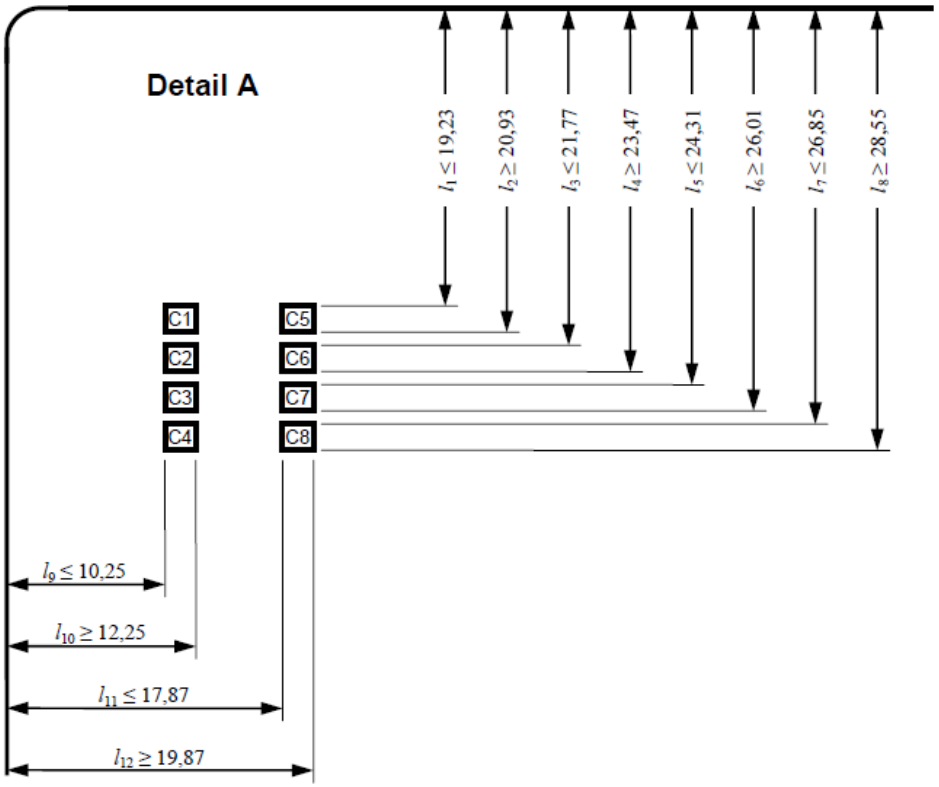


Fig.8 - Localização dos contatos

4 Estudo de modelos de *chips* para eID existentes no mercado

Nesta seção iremos apresentar as características de alguns chips para eID mais comumente encontrados no mercado. Atualmente, dois fabricantes, a Infineon e a NXP, que mais se destacam nos produtos de eID e smartcards, por apresentarem soluções mais completas em relação aos critérios de segurança do hardware e dos dados armazenados. Mas outros fabricantes como ST Microelectronics e Samsung também produzem chips para eIDs. Esta segurança da informação é garantida através de recursos como co-processador com algoritmos de criptografia, e certificada por critérios de homologação de segurança, como o *Common Criteria*, FIPS 140-2 e o EMV, que serão descritos na seção seguinte.

Os chips com microprocessadores utilizados em Smartcards são específicos para cada aplicação, ou seja, não são utilizados os processadores "padrões" largamente utilizados pela indústria eletrônica de consumo. Os motivos desta especificidade do microprocessador são: custo de fabricação, funcionalidade (coprocessador criptográfico,

segurança) e área do silício (chip) limitada pelo cartão. Algumas características são essenciais para definirmos o chip adequado a uma determinada aplicação e seus recursos, como: Interface de comunicação, processador lógico (CPU), tipos e tamanhos das memórias, co-processador criptográfico, gerador de números aleatórios (RNG) e unidade de gerenciamento de memória (MMU).

As interface de comunicação com o leitor externo podem definidas como com-contato (*contact*) ou sem-contato (*contactless*). As memórias podem ser definidas como não-volátil (ROM, EEPROM ou Flash) ou volátil (RAM). A memória ROM (*Ready Only Memory*) armazena o software do Sistema Operacional e, por vezes, algumas *applets*, por meio de instruções binárias de controle da CPU, e funções da memória não volátil EEPROM ou Flash. As memórias EEPROM (*Electrically Erasable Programmable Read Only Memory*) ou Flash são utilizadas para o armazenamento seguro de dados personalizados, de informações secretas como por exemplo, chaves de criptografia (*encryption keys*), certificados de segurança, e eventualmente de alguns *applets* inseridos após a fabricação. Já a memória RAM (*Random Acess Memory*) mantém os dados somente quando aplicada uma tensão de alimentação no chip e é utilizada pelo processador como uma memória operacional que armazena variáveis, resultados intermediários e dados de interface. A vantagem da memória RAM é a rapidez de leitura e escrita, porém, ocupa uma área de silício bem maior que uma memória ROM. Os co-processadores implementam os algoritmos de criptografia, como o DES, o AES, o RSA e a curva-elíptica. A diferença entre co-processador criptográfico e o processador lógico é que o criptográfico possui uma alta eficiência com relação a cálculos matemáticos necessários para as funções de criptografia.

Por fim, os chips de SmartCard apresentam, implementado fisicamente em hardware, um gerador de números aleatórios (RNG), que representa uma função essencial para a segurança dos protocolos criptográficos.

A seguir são listados alguns chips produzidos para a aplicação em eIDs.

4.1 Infineon - Portfólio de *Chips* para segurança e *Smart Cards* (*Secure eGovernment*) [6]

Tab. 3 - Portfólio de Chips da Infineon para eGovernment

***Dual-Interface* e *Contactless* (sem-contato)**						
Produto	**Memória**	**CPU**	**Crypto coprocessador**	**Interfaces**	**Certificação**	**Aplicações**
SLE 66CLX1600PE (M/S)	EEPROM 160kByte ROM 240kByte XRAM 6kByte Crypto700Byte IRAM 256Byte	8-bit 16-bit	3DES RSA 2048-bit ECC 521-bit	ISO 7816 ISO14443 A/B ISO18092 (modo passivo) Mifare	CC EAL5+	*National eID ePassport eHealth card eSocial card eDriver's License eVisa eResidence Permit, eCar Registration eSignature*
SLE 78CLX1600P	EEPROM 160kByte ROM 280kByte RAM 8kByte	Dual 16-bit	DES 3DES AES 256-bit RSA 4096-bit ECC 521-bit	ISO 7816 ISO14443 A/B ISO18092 (modo passivo) Mifare	CC EAL5+ EMVCo	*National eID ePassport eHealth card eSocial card eDriver's License eVisa eResidence Permit, eTachograph eCar Registration eSignature*
SLE 78CLFX5000PH	SOLID FLASH 500kByte RAM 12kByte	Dual 16-bit	DES 3DES AES 256-bit RSA 4096-bit ECC 521-bit	ISO 7816 ISO 14443 A/B ISO 18092 (modo passivo) Mifare	CC EAL6+ EMVCo	*National eID ePassport eHealth card eSocial card eDriver's License eVisa eResidence Permit, eTachograph eCar Registration eSignature*
SLE 78CLFX500VPH	SOLID FLASH 500kByte RAM 12kByte	Dual 16-bit	DES 3DES AES 256-bit RSA 4096-bit ECC 521-bit	ISO 7816 ISO14443 A/B ISO18092 (modo passivo) Mifare VHBR	CC EAL6+ EMVCo	*National eID ePassport eHealth card eSocial card eDriver's License eVisa eResidence Permit, eTachograph eCar Registration eSignature*
Contactless (sem-contato)						

SLE 77CLF1001P	SOLID FLASH 100kByte RAM kByte	16-bit	DES 3DES AES 256-bit	ISO 7816 ISO14443 A/B ISO18092 (modo passivo) Mifare	CC EAL5+ EMVCo	*National eID* *eHealth card* *eSocial card* *eDriver's License* *eCar Registration*
***Contact-based* (com-contato)**						
SLE 77CF1200S	SOLID FLASH 120kByte RAM4kByte	16-bit	DES AES	ISO 7816	EMVCo	*National eID* *eHealth card* *eSocial card*
SLE 77CFX2400P	SOLID FLASH 240kByte RAM6kByte	16-bit	DES 3DES AES 256-bit RSA 4096-bit ECC 521-bit	ISO 7816	CC EAL5+ EMVCo	*National eID* *eHealth card* *eSocial card* *eDriver's License* *eTachograph* *eCar Registration*
SLE 78CX1600P	EEPROM 160kB ROM288kB RAM8kB	Dual 16-bit	3DES AES 256-bit RSA 4096-bit ECC 521-bit	ISO 7816	CC EAL5+ EMVCo	*National eID* *eHealth card* *eSocial card* *eDriver's License* *eTachograph* *eCar Registration* *eSignature*
SLE 78CFX5000PH	SOLID FLASH 500kByte RAM 12kByte	Dual 16-bit	DES 3DES AES 256-bit RSA 4096-bit ECC 521-bit	ISO 7816	CC EAL6+ EMVCo	*National eID* *eHealth card* *eSocial card* *eDriver's License* *eTachograph* *eCar Registration* *eSignature*

4.2 Infineon - Pacotes para *Secure eGovernment*

Tab. 4 - Pacotes completos da Infineon para eGovernment

***Dual-Interface* e *Contactless* (sem-contato)**						
Produto	**Memória**	**Padrões**	**Crypto coprocessador**	**Interfaces**	**Certificação**	**Aplicações**
SLN 52GDA128 DM (*Native Generic ID Platform*)	EEPROM 36kB 80kB 128kB	ICAO BAC, SAC, AA BSI-TR03110 v1.11 and v2.05 EAC ISO 7816-4, 8,9 ISO 18013 BAP, EAP config1-4	DES 3DES AES 256-bit RSA 4096-bit ECC 521-bit	ISO 7816 ISO 14443 A/B OS Provider: Masktech - MTCOS	CC EAL4+	*National eID ePassport eHealth card eSocial card eDriver's License eVisa eResidence Permit, eCar Registration eSignature*
PCL16MCOS01ID (*Native Basic ID Platform*)	EEPROM 8kByte 16kByte	ISO 7816-4, 8, 9 ISO 18013 BAP config1-4	DES 3DES	ISO 7816 ISO 14443 A/B OS *Provider:* *Masktech* - MTCOS		*National eID ePassport eHealth card eSocial card eDriver's License eVisa eResidence Permit, eCar Registration*
SLJ 52GDL128 DL *JavaCard Platform, including ePassport & eSign Applet*	EEPROM 36kByte 80kByte 128kByte	JC 3.0 GP 2.2 ICAO BAC, SAC, AA BSI-TR03110 v1.11 EAC ISO 18013 BAP, EAP config1-4	DES 3DES AES 256-bit RSA 4096-bit ECC 521-bit	ISO 7816 ISO 14443 A/B Mifare OS Provider: Trusted Logic - jTOP	CC EAL5+	*National eID ePassport eHealth card eSocial card eDriver's License eVisa eResidence Permit, eCar Registration eSignature*
JCL X80jTOP31IDv2 *JavaCard Platform, including ePassport Applet*	EEPROM 36kByte 80kByte	JC 2.2.1 GP 2.1.1 ICAO BAC, AA, BSI-TR03110 v1.11 EAC ISO 18013	DES 3DES AES 128-bit RSA 2048-bit ECC 521-bit	ISO 7816 ISO 14443 A/B OS Provider: Trusted Logic - jTOP	CC EAL5+	*National eID ePassport eHealth card eSocial card eDriver's License eVisa eResidence Permit, eCar Registration eSignature*

		BAP, EAP config1				

4.3 NXP - Portfólio de *Chips* para segurança e *Smart Cards* (*Secure eGovernment*)

Emprego de microprocessadores SmartMX e SmartMX2 com certificação CC EAL 5+ / CC EAL 6+.

Tab. 5 - Portfólio de Chips da NXP para eGovernment

***Dual-Interface* e *Contactless* (sem-contato)**					
Produto	**Memória**	**Crypto coprocessador**	**Interfaces**	**Certificação**	**Aplicações**
SmartMX	EEPROM 8kB to 144kByte (Retenção de dados: 25 anos; 500.000 ciclos) ROM [160-264] kB RAM [3.5Kb- 7.5]kB MMU	3DES (64-bit) AES (128-bit) PKI (RSA, ECC) (32-bit)	ISO 7816 ISO 14443 A/B MIFARE DESFire MIFARE Classic MIFARE FleX	CC EAL5+ EMVCo	*National eID ePassport eHealth card eSocial card eDriver's License eVisa eResidence Permit, eCar Registration eSignature; Public Transport; Banking*

4.4 Exemplos de Chips utilizados em soluções de eID nacionais

Com o objetivo de analisar as soluções de mercado adequadas à aplicação de eIDs, e com base nisso poder especificar parâmetros e níveis de segurança compatíveis com o que é ofertado pelo mercado, ilustramos a Tabela 6 extraída do RT de Diagnostico de Tecnologias de Identidades, com dados sobre os chips e sistemas operacionais utilizados nas eIDs nacionais.

Tabela 6 : Especificação dos chips e sistemas operacionais empregados em eIDs nacionais.

País	Modelo / Nível de segurança/ recurso de proteção	Memórias	Processador/ Coproc.	Ref
Bélgica	SLE66CX360PE BSI-PP0002 EAL 5+ CRC, MMU, ECU	240KB ROM, 7KB RAM, 6KB EEPROM, RSA(2048), 3DES(112), DSA(512)	Proc: 16 bit Coproc: - Crypto 1100bit (RSA) -112bit crypto acc. DES - RSA 1024-Exp.65537 - Não calcula hash internamente	[18] [19] [20] [21]
Espanha DNI 3.0	EAL6+	Memória flash RAM: 64kB	Proc: 32bits Coproc: - ECC - AES - SHA-2	[22]
Portugal	CC/SLE66CX322P BSI-PP0002 EAL 5+	136KB ROM, 5KB RAM, 32KB EEPROM, RSA(2048), DSA(1024), ECC(192), True RNG	Proc: 16bits Coproc: - RSA - DES	[23] [24]
Eslovênia HIC	SamsungS3CC91C BSI-PP0002 EAL 4+	72KB Flash, 72KB EEPROM, 384KB ROM, 10KB RAM		[24]
Espanha DNI 2.0	ST19wl34 BSI-PP0002 EAL5+, CRC	224KB ROM, 6KB RAM, 34KB EEPROM, RSA(2048)		[22] [23] [24] [25]

O risco de emprego de chips de uso genérico, como chips de Pay-TV amplamente atacados, para aplicações mais críticas como eID é citado em [16]. Alguns

requisitos especificados para eID´s de alguns países confirmam a tendência de emprego de níveis de segurança EAL 5 ou superior: Áustria (EAL 5+) e Espanha-DNI3 (EAL6+). Observa-se que, dentre os chips identificados, o padrão de proteção PP BSI-PP0002 de 2001 é o mais aplicado.

Também são apresentados alguns exemplos de chips de smartcards aplicados em soluções recentes de eID nacionais. No entanto, vale ressaltar que em alguns países foram contratadas soluções definidas como "pacote fechado", ou seja, não houve um projeto nacional de especificação da solução adequada e nem definição dos chips a serem utilizadas nesta aplicação em eID. Portanto, serão apresentadas somente algumas características gerais dos chips aplicados aos eID´s nacionais, devido a esta falta de informação específica sobre o chip utilizado no smartcard.

4.4.1 eID do Uruguai

No eID do Uruguai [13] foi contratada uma empresa que fornecesse a solução completa (pacote fechado) de eID, definindo tanto o smartcard quanto os chips utilizados. Abaixo estão descritas algumas características desta solução:

- Durabilidade dos documentos de 5 a 10 anos;
- Cartão de policarbonato;
- Sistema de personalização descentralizado;
- Solução com 2 chips: Com contato e Sem contato;
- Aplicações eGov e ICAO;

Pacote *Sealys eID card*

Chip com contato:

- Aplicação Match on Card (MoC):
  - Autenticação de identidade (impressão digital)
  - Atende os patrões biométricos da ISO197942
  - Armazena com segurança e compara até 10 padrões biométricos (recomendação 2-4 padrões biométricos)
- Aplicação PKI:
  - Assinatura digital;

- Armazena informações biográficas em estruturas da ISO7816 e certificados digitais com RSA e ECC;
- Permite autenticação e assinatura digital com chaves RSA e ECC

Chip sem contato

- Aplicação ICAO:
  - Documento de viagem dentro do Mercosul;
  - Modo BAC;

Sistemas Coesys Issuance solution

Combinação de serviços de software, hardware e integração, de personalização de documentos seguros como eID e ePassaport;

Normas e padrões:

-ISO/IEC 7816, ISO/IEC, 14443 ISO/IEC 19794, ISO 17799/ ISO 27001;

- Global Plataform/JavaCard,Multos;
- ICAO Doc 9303;
- IAS Specification; IAS v1.01 Premium;
- PIV/FIPS 201 aprovado pela GSA, HSM FIPS 140-2 Level 3;
- RSA Labs. PKCS #1-15;
- BS 7799;
- Aplicações: ICAO LDS 1.7 e PKI 1.1(AA e EAC);
- EMV.

4.4.2 eID de Bangladesh

A eID de Bangladesh [14] foi contratada uma empresa que fornecesse a solução completa, sem uma especificação detalhada do smartcard e dos chips utilizados. A seguir são descritas algumas informações do sistema de eID implementado neste país:

Especificações técnicas do SmartCard:

- Policarbonato, conforme normas ISO/IEC 7810, 7816 e 10373-1;
- Testes em laboratórios certificados com ISO 17025:2005;
- Durabilidade mínima de 10 anos;
- Espessura de 760um +/- 80um;
- Personalização gráfica *below-surface* e *on-surface laser engraving*;

- Sistema Operacional Nativo ou JavaCard;
- Padrão ISO/IEC 7810 e ISO/IEC 7816 (Chip com contato);
- Certificação Fogra AGE F02 (*artificial ageing*);

Especificações técnicas do Chip:

- Memória de dados > 60Kb (foto, chaves, dados pessoais, etc);
- Coprocessador: DES; 3DES, CRC;
- Certificação mínima Common Criteria EAL 4+;
- Interface COM CONTATO, de acordo com o padrão ISO/IEC 7816-3;
- Protocolo T=0 e T-1;
- Gerador de Números Aleatórios Real (True RNG);
- O chip deve suportar pelo menos 100.000 ciclos de escrita.

5 Critérios e Homologação de segurança

Os Smartcards são dispositivos de segurança portáteis, que podem armazenar de forma segura informações pessoais e confidenciais. Além disso, os smartcards devem permitir transações seguras, validar a identidade de um indivíduo dentro de um sistema seguro, e verificar se uma solicitação está autorizada a acessar a informação armazenada no cartão. Portanto, os smartcards devem não só manter a integridade da informação armazenada no cartão, mas também torná-lo disponível para consultas e transações das informações com o sistema geral.

Geralmente, o nível de segurança é aceitável quando o o custo de um ataque bem sucedido é uma ordem de grandeza superior ao valor agregado da informação protegida [15]. Os ataques são técnicas implementadas para comprometer a segurança de um Circuito Integrado de um smartcard. Os ataques podem ser classificados como ataques de falha (fault attacks) , ataques de canal lateral (side-channel attacks), ou ataques invasivo (invasive attacks).

Ataques de Falha altera o funcionamento interno do CI para induzir um erro na operação do mesmo, revelando inormações importantes sobre o circuito integrado. Conforme apresentado anteriormente, na seção 3.4, um chip de segurança possue sensores que controlam a operação do circuito nos limites extremos de operação definos durante a especificação e projeto do chip. Ou seja, se o CI é manipulado para funcionar

fora dos parâmetros previamente estabelecidos, o CI passa para o modo de cancelamento completo de seu funcionamento.

Ataques de canal lateral são ataques com base em informações obtidas a partir da implementação física de um sistema de criptografia. Muitas informações internas podem ser obtidas afim de se explorar a quebra do sistema. Muitos ataques de canal lateral requer considerável conhecimento técnico do funcionamento interno do sistema e da criptografia a ser implementada.

Por fim, ataques invasivos, também conhecidos como ataques de hardware, usam meios mais intrusivos para acessar as informações sobre o chip. Um exemplo de ataque invasivo seria a análise detalhada do chip utilizando um ultrasom (ou microprobe) ou um feixe de íons, permitindo assim, uma engenheria reversa de todo o circuito integrado e, consequentemente, uma alteração do sistema. Felizmente, algumas medidas defensivas podem ser implementadas em um CI para evitar estes ataques invasivos [15].

Devido a grande complexidade e diversidade de ataques físicos e recursos de proteção de smartcards, alguns países, por meio de instituições de pesquisa na área de segurança da informação passaram a realizar os serviços de certificação de segurança, com a formalização dos testes. Além disso, entidades privadas também passaram a oferecer tais serviços, mas sem o mesmo nível de formalismo dos testes. Dessa forma, o uso destes certificados é uma forma eficaz de especificar requisitos de segurança de um chip, de acordo com a aplicação. Alguns esquemas proprietários são aplicados principalmente para cartões bancários (EMV). Para eIDs, que utilizam requisitos mais fortes de segurança, são aplicados em geral esquemas padronizados formalmente, como Common Criteria (ISO/IEC 15408) e FIPS 140-2, os quais são detalhados a seguir.

5.1 Common Criteria (CC)

Common Criteria (CC) [4] é um certificado para Segurança de produtos e sistemas da Tecnologia da Informação (*Information Technology Security*). É um padrão desenvolvido por um grupo de institutos nacionais ligados à pesquisa de segurança da informação (CRCA- *Common Criteria Recognition Arrangement*)), absorvido pela norma internacional, ISO/IEC 15408, a qual define a segurança para os sistemas computacionais e de informação voltados para a segurança lógica e desenvolvimento de aplicações seguras. A

versão atual é a versão 3.1 revisão 4. Este padrão define um método para avaliação da segurança de ambientes de desenvolvimento de sistemas e visa desenvolver níveis de segurança que determinam os requisitos (*Security Assurance Requirements – SARs*) e funções de segurança (*Security Functional – SFRs*) para um determinado sistema de informação.

O CC foi desenvolvido combinando padrões de segurança de vários países. O CC estabelece e mantém padrões rigorosos para os critérios de avaliação e execução de testes laboratoriais. Os testes e validações feitas por laboratórios credenciados são verificados pelo órgão do *Common Criteria* do país em questão.

Governos de 26 países ratificaram um acordo de reconhecimento do CC (*CCRA-Common Criteria Recognition Arrangement*) como padrão de avaliação de segurança. Existem dois tipos de membros do CC, os *Certificate Authorizing Members (CAM)*, que são capazes de certificar os sistemas, e os *Certificate Consuming Members (CCM)*, que aceitam os certificados do CC como padrões de segurança nos sistemas de TI.

- Países membros do CAM:
  - Austrália, Canada, França, Alemanha, Índia, Itália, Japão, Malásia, Holanda, Nova Zelândia, Noruega, Coreia do Sul, Espanha, Suécia, Turquia, Reino Unido, Estados Unidos;
- Países membros do CCM:
  - Áustria, República checa, Dinamarca, Finlandia, Grécia, Hungria, Israel, Paquistão, Singapura;

Diferente do FIPS140, o CC não define uma lista de requisitos/recursos de segurança de um produto específico. Os fabricantes ou clientes especificam os próprios requisitos através de critérios bem definidos e laboratórios credenciados certificam/validam se os produtos atenderam aos atributos de segurança especificados. As especificações de segurança são feitas através dos padrões de proteção (*Protection Profile*-PP). Portanto, o CC basicamente garante que os processos de especificação, implementação e validação sejam conduzidos de maneira formal e rigorosa.

Termos gerais

O CC possui diversos elementos:

- ***Target of Evaluation* (TOE):** produto ou sistema sujeito à Avaliação;

O CC é flexível no que diz respeito ao "objeto" ou "alvo" a ser avaliado, sendo utilizado o termo TOE. O TOE pode ser definido como um conjunto de software, firmware e/ou hardware. Portanto, o TOE pode ser definido como um produto de TI, uma parte de um produto, um conjunto de produtos, uma tecnologia empregada em um produto de TI ou uma combinação de todos estes.

Exemplos de TOEs incluem: software de aplicação; sistema operacional; um sistema operacional combinado com uma estação de trabalho (*workstation*); um circuito integrado de um smart card; um co-processador criptográfico; todos os componentes de uma rede local (*Local Area Network* - LAN), incluindo terminais, servidores, equipamentos de rede e software; aplicações de banco de dados.

A avaliação serve para validar reivindicações feitas sobre o *target* (alvo). Para ser de uso prático, a avaliação deve verificar os recursos de segurança do alvo. Isto é feito através do seguinte:

- ***Protection Profile* (PP):** documento elaborado pelo usuário ou por uma comunidade técnica que descreve os requisitos de segurança para um produto/sistema (TOE) específico. Os requisitos de segurança dos consumidores são descritos neste documento, que representa uma estrutura independente da implementação.
- ***Security Target* (ST):** documento que especifica as propriedades de segurança do TOE. Os requisitos de segurança exigidos pelos consumidores e atendidos pelos produtos gerados pelos desenvolvedores estão descritos no *Security Target* (ST), em uma estrutura dependente da implementação. Este documento auxilia os desenvolvedores durante o processo de desenvolvimento de seus

produtos e nas avaliações de segurança de seus TOE´s. Este documento ST pode ser baseado em um ou mais PPs afim de se demostrar que o ST está em conformidade com o requisitos de segurança dos consumidores, tal como estabelecido nos PPs. A ST é geralmente publicado para que os potenciais clientes possam determinar as características de segurança específicas que tenham sido certificados pela avaliação.

- ***Security Functional Requiriments* (SFRs):** documento que define as funções de segurança fornecidas pelo produto. Os documentos do CC apresentam um catálogo padrão das funções de segurança. A lista de SFRs pode variar de uma avaliação para outra, mesmo sendo definidas para um mesmo tipo de produto. Ou seja, o CC não descreve as SFRs a serem incluídas em uma ST. No entanto, identifica as dependências de uma certa função de segurança para o correto funcionamento de uma função dentro de um único produto.

Além disso, o processo de avaliação também tenta determinar o nível de confiança que pode ser colocada nos recursos de segurança do produto por meio de processos de garantia de qualidade:

- ***Security Assurance Requirements* (SARs):** descrição das medidas tomadas durante o desenvolvimento e avaliação do produto para garantir a conformidade com a funcionalidade de segurança reivindicada.

- ***Evaluation Assurance Level* (EAL):** Define a “conformidade” dos requisitos qualificados durante a avaliação. Cada EAL corresponde a um pacote de requisitos garantidos no desenvolvimento e testes do produto.

O CC define7 níveis de avaliação de segurança: EAL1 até o EAL7, conforme apresentado na Tab. 7.Um nível maior não implica em uma melhor segurança, apenas indica que o produto foi avaliado por um processo mais rigoroso.

- Os níveis de EAL definem o grau de confiabilidade do TOE no contexto de uma avaliação;

- A quantidade de esforço aumenta de forma quase quadrática (não linear) de um nível para outro. Ou seja, requer o dobro de esforço para passar de um nível para o seguinte;
- Uma avaliação EAL7 pode levar vários anos e custar vários milhões de euros;

Tab.7 - Descrições dos níveis de EAL1 até o EAL7. Fonte [4] .

Criterion	Description
EAL1	Functionally tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Jethodically designed, tested, and reviewed
EAL5	Semiformally designed and tested
EAL6	Semiformally verified design and tested
EAL7	Formally verified design and tested

- ***Evaluation assurance level 1 (EAL1) – functionally tested***

- O EAL1 é aplicável quando é necessária alguma confiança na operação correta, mas as ameaças à segurança não são vistas como graves. Neste nível, a proteção é exercida sobre os dados pessoais ou informações similares.

- O EAL1 fornece um nível básico de segurança para uma meta de segurança limitada. Ou seja, é realizada uma análise das funções de segurança (SFRs) através dos requisitos de segurança (ST) afim de procurar potenciais de vulnerabilidades no domínio público, independente de testes funcionais.

- Evaluation assurance level 2 (EAL2) – structurally tested

- O EAL2 requer a cooperação do desenvolvedor nos termos da entrega do projeto e dos resultados dos testes.

- O EAL2 é, portanto, aplicável nas circunstâncias em que os desenvolvedores ou usuários requerem um nível baixo ou moderado de segurança de forma independente, na ausência de disponibilidade imediata do registro completo do desenvolvimento.

- O EAL2 fornece a garantia de uma meta de segurança completa e uma análise das funções de segurança (SFRs) e dos requisitos (ST), utilizando especificações funcionais e de interface e uma descrição básica da arquitetura do TOE, para entender o comportamento de segurança.

- O EAL2 também fornece uma garantia por meio do uso de um sistema de gerenciamento das configurações do sistema e uma comprovação dos procedimentos de entrega segura das informações. Este EAL representa um aumento significativo na garantia de segurança comparando com ao EAL1 através de testes do desenvolvedor, uma análise de vulnerabilidade, e testes independentes baseados em especificações mais detalhadas da TOE.

- ***Evaluation assurance level 3 (EAL3) – methodically tested and checked***

- O EAL3 permite que um desenvolvedor obtenha uma garantia máxima de engenharia de segurança na fase de concepção, sem alteração substancial nas práticas sólidas de desenvolvimento existentes.

- O EAL3 é aplicável nos casos em que os desenvolvedores ou usuários requerem um nível moderado de segurança de forma independente assegurada, e exigem uma profunda investigação do TOE e do seu desenvolvimento sem necessidade de umareengenharia substancial.

- Evaluation assurance level 4 (EAL4) – methodically designed, tested, and reviewed

- O EAL4 permite que um desenvolvedor obtenha uma garantia máxima de segurança com base nas boas práticas de desenvolvimento comerciais que, embora rigorosas, não requerem conhecimento substancial de especialistas,

habilidades e outros recursos. O EAL4 é em geral o nível mais alto para o qual seja economicamente viável a certificação de uma linha de produtos existente.

- O EAL4 é, portanto, aplicável nas circunstâncias em que os desenvolvedores ou usuários requerem um moderado a alto nível de segurança de forma independente assegurada em TOEs convencionais, e que estejam dispostos a custear serviços de engenharia específicos para uma segurança adicional.

- Evaluation assurance level 5 (EAL5) - semiformally designed and tested

- O EAL5 permite que um desenvolvedor obtenha uma garantia máxima de engenharia de segurança com base em práticas de desenvolvimento comerciais rigorosas, apoiados por uma moderada aplicação de técnicas especializadas de engenharia de segurança. Cada TOE vai provavelmente ser com a intenção de alcançar a garantia EAL5. É provável que os custos adicionais, (com relação aos nívies anteriores EAL1 ao ELA4), relativos aos requisitos do EAL5, devido ao desenvolvimento rigoroso sem a aplicação de técnicas especializadas, não seja grande.

- O EAL5 é, portanto, aplicável nas circunstâncias em que os desenvolvedores ou usuários requerem um elevado nível de segurança de forma independente em um desenvolvimento planejado e exigem uma abordagem de desenvolvimento rigorosa, sem incorrer em custos excessivos atribuíveis a técnicas especializadas de engenharia de segurança.

- Evaluation assurance level 6 (EAL6) – semiformally verified design and tested

- O EAL6 permite aos desenvolvedores obter uma alta garantia na aplicação de técnicas de segurança para um ambiente rigoroso de desenvolvimento, afim de produzir um TOE para proteger os ativos de alto valor, contra riscos significativos.

- O EAL6 é, portanto, aplicável ao desenvolvimento de TOEs de segurança para aplicação em situações de alto risco, onde o valor dos ativos justifica o custo adicional de certificação.

- ***Evaluation assurance level 7 (EAL7) - formally verified design and tested***

  - O EAL7 é aplicável ao desenvolvimento de TOEs de segurança para aplicação em situações de risco extremamente elevado e/ou onde o alto valor dos ativos justifica os custos mais elevados de certificação.

Além dos níveis de avaliação, existe a robustez (força) dos mecanismos contra ataques. São definidos 3 pontos da robustez: baixo (*low*), médio (*medium*) e alto (*high*);

- *Low*: proteção contra ataques aleatórios;
- *Medium*: proteção contra ataques com recursos limitados;
- *High*: (EAL4+ ou EAL5+) proteção contra atacantes com recursos técnicos e bons conhecimentos. Ex: Microcontroladores para Smartcards e sistemas operacionais

A Fig. 9 representa os requisitos de segurança (*assurance requirements*) através das clases e familia de segurança. Além disso, é apresentada a estrutura destas famílias de segurança.

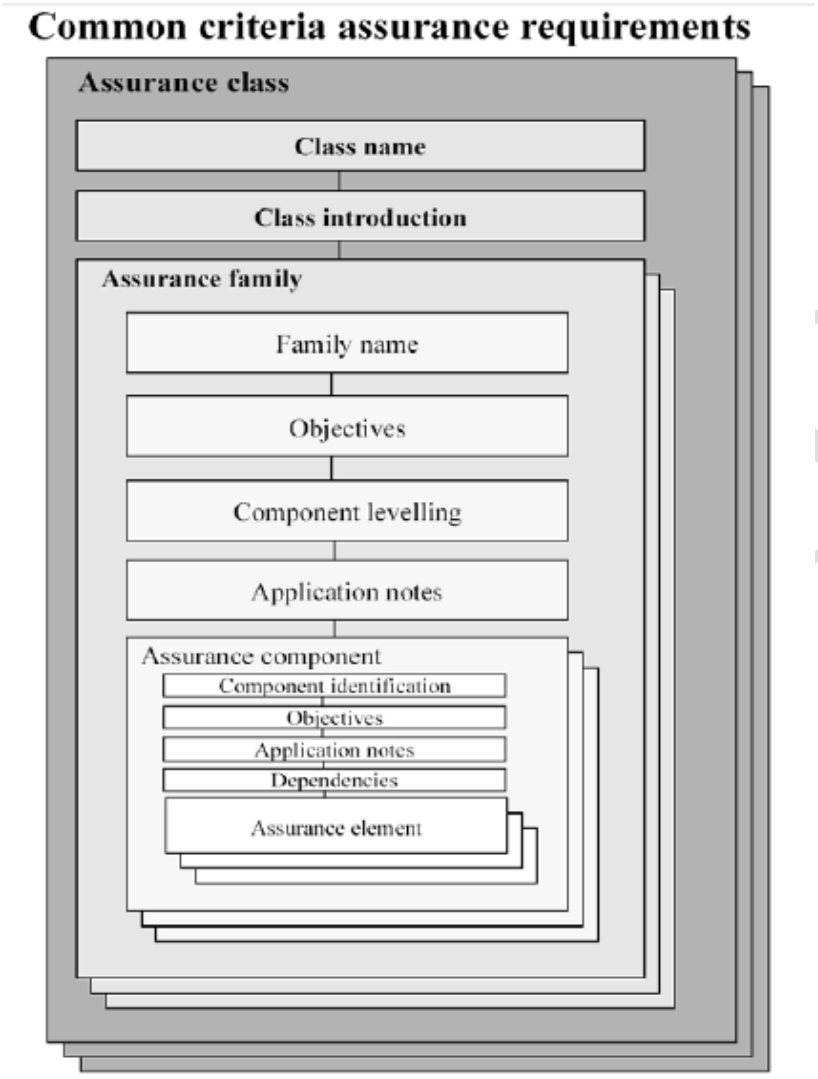


Fig.9 - Requisitos de segurança do CC e estrutura das famílias de segurança. Fonte [4]

Na Tabela 8, são apresentados as classes, as famílias e os níveis de segurança correspondentes. Note que, dependendo da familía de segurança, os níveis de segurança dos componentes podem ser iguais ou maiores de acordo com os diferentes níveis EAL. Por exemplo, para a classe de Desenvolvimento (*Development*) e família ADV_ARC, os níveis de EAL2 até o EAL7 apresentam o mesmo nível de segurança, igual a 1. Ao passo, que para a classe de Vunerabilidade (*Vulnerability*) e família AVA_VAN, diferentes níveis EAL apresentam diferentes níveis de segurança, nível 1 para o ELA1 e nível 5 para os níveis EAL6 e EAL7. Portanto, através desta tabela podemos verificar os valores dos níveis de segurança de cada classe e família para os diferentes níveis EALs.

Tab.8 - Classes, famílias e níveis de segurança EAL1 até EAL7. Fonte [4].

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Documentação

A documentação básica do CC é definida em 3 partes:

Parte 1 – "*Introduction and General Model*": descreve as características e definições básicas da avaliação do CC; especifica o TOE (*Target Of Evaluation* – Alvo de Avaliação) e o PP (*Protection Profile* - Perfil de Proteção)

Parte 2 – "*Security functional requirements*": descreve os requisitos funcionais de segurança; lista das exigências sobre a funcionalidade do alvo (*target*) de avaliação.

Parte 3 – "*Security assurance requirements*": consiste em descrições detalhadas dos requisitos de garantia de segurança, EAL (*Evaluation Assurance Levels* – Níveis de garantia de avaliação).

A tabela 9 descreve a importância de cada parte do CC para os três grupos interessados na avaliação das propriedades de segurança de um TOE: Consumidores, Desenvolvedores e Avaliadores.

Tab.9 - Relevância das partes do CC para os três grupos de usuários. Fonte [4].

	Consumers	Developers	Evaluators
Part 1	Use for background information and are obliged to use for reference purposes. Guidance structure for PPs.	Use for background information and reference purposes. Are obliged to use for the development of security specifications for TOEs.	Are obliged to use for reference purposes and for guidance in the structure for PPs and STs.
Part 2	Use for guidance and reference when formulating statements of requirements for a TOE.	Are obliged to use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Are obliged to use for reference when interpreting statements of functional requirements.
Part 3	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use for reference when interpreting statements of assurance requirements.

Consumidor: os documentos do CC são descritos para que a avaliação de segurança de um determinado TOE atenda às necessidades dos consumidores, sendo assim, uma justificativa e um propósito fundamental do processo de avaliação. Os requisitos de segurança dos consumidores são descritos em uma estrutura independente da implementação, denominada *Protection Profile (PP).*

Desenvolvedores: Os documentos do CC se destinam a apoiar os desenvolvedores na preparação e assistência durante as avaliações de segurança de seus TOE´s e na identificação de que os requisitos de segurança exigidos pelos consumidores foram atendidos. Estes requisitos de segurança estão contidos em um documento dependende da implementação denominado *Security Target (ST).* Este ST pode ser baseado em um ou mais PPs para mostrar que o ST está em conformidade com o requisitos de segurança dos consumidores, tal como estabelecido nos PPs.

Avaliadores: Os documentos do CC contém critérios utilizados pelos avaliadores no intuito de analisar as conformidades dos TOE´s com os respectivos requisitos de segurança exigidos pelo PP. O CC descreve um conjunto de ações gerais a serem executadas pelos avaliadores. No entanto, o CC não define procedimentos específicos a serem seguidos.

Modelo Geral

Nesta seção serão descritos os conceitos básicos através de um modelo geral do Common Criteria.

Ativos e Contramedidas (*Assets and Countermeasures*): Critérios de segurança são necessários para a proteção de ativos (*assets*). Pode se definir ativos de várias maneiras, como por exemplo, um conteúdo de um arquivo ou servidor, autenticação de votos em uma eleição ou acesso restrito à um equipamento o rede. Além disso, podemos definir ativos na forma de informação que é gravada, processada e transmitida por um produto de TI. Proprietários (*owners*) destas informações podem exigir que a disponibilidade, divulgação e modificação de tais informações são rigorosamente controladas e que os ativos estão protegidos contra ameaças (*threats*) através de contramedidas (*countermeasures*), reduzindo assim os riscos (*risk*) de ataques, conforme apresentado na figura abaixo.

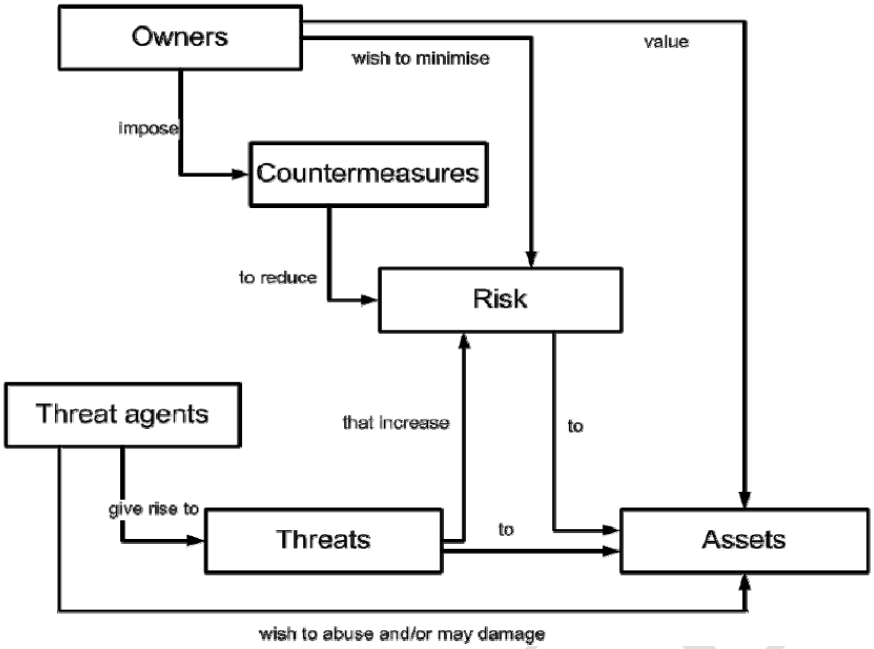


Fig.10 Conceitos de segurança. Fonte (retirado) [4].

Os proprietários dos ativos são os responsáveis por eles, portanto, deverão ser capazes de implementar contramedidas e defendê-los contra os riscos e aceitar, através de critérios de segurança, alguns níveis de exposição dos ativos a ameaças.

Dois elementos importantes devem ser levados em consideração durante a análise de uma contramedida contra riscos:

- **Se as contramedidas são suficientes**: se as ameaças aos ativos são combatidas adequadamente com as contramedidas implementadas. A suficiência de uma contramedida é definida no ST (*Security Target*).

O documento ST divide as contramedidas em dois grupos principais: Objetivos de segurança do TOE (a correção das contramedidas serão determinadas na avaliação) e objetivos de segurança para o ambiente operacional no qual o ativo está localizado (a correção das contramedidas não é determinada na avaliação, pois existem condições externas não controláveis). Por fim, o ST requer um detalhamento maior dos obetivos de segurança do TOE no documento *Security Functional Requirements* (SFRs).

- **Se as contramedidas são corretas**: se as contramedidas aumentam a proteção dos ativos às ameaças e riscos que elas deveriam combater.

Uma contramedida (ou definida na avaliação como TOE) pode ser incorretamente projetada e implementada, e pode, portanto, conter erros que levem a vulnerabilidades e ataques aos ativos. O documento ST fornece uma descrição estruturada das atividades e testes a serem executadas, afim de se determinar a correta implementação das contramedidas, na forma do *Security Assurance Requirements* (SAR).

No entanto, muitos proprietários de ativos não têm o conhecimento, a experiência ou os recursos necessários para julgar a suficiência e exactidão das contramedidas. Portanto, conforme demonstrado na Fig.11, estes proprietários podem solicitar uma avaliação (*Evaluation*) externa para aumentar a sua confiança (*Confidence*) na suficiência (Sufficient) e correção (*Correct*) das contramedidas implementadas.

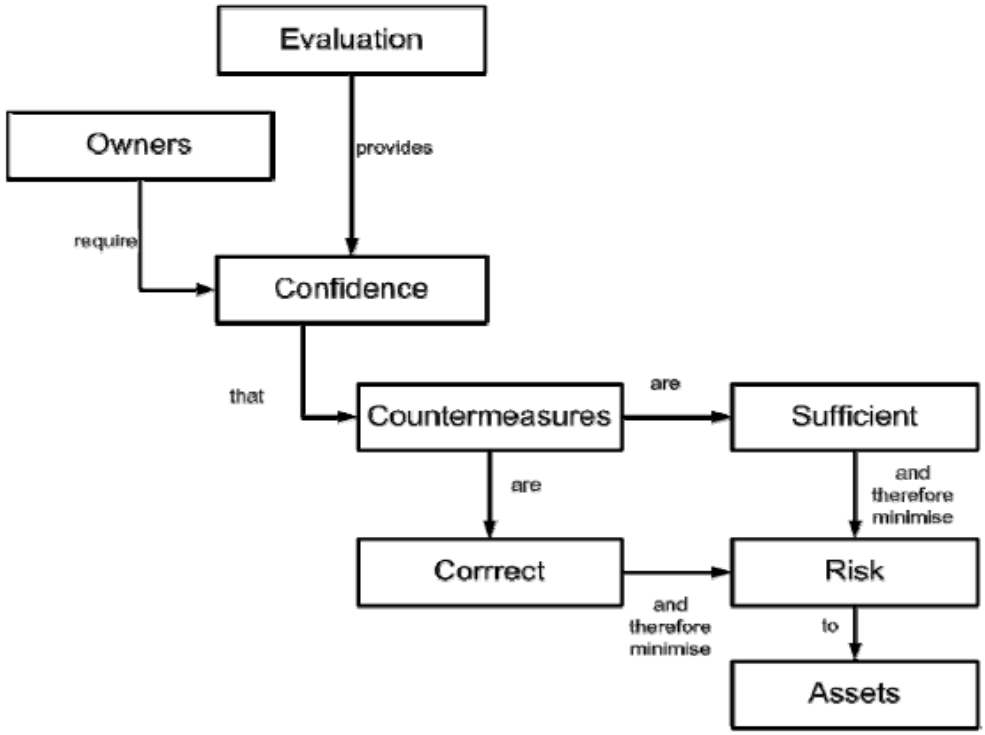


Fig.11 Conceitos de avaliação de segurança. Fonte [4].

Na Tab.10 são apresentados os documentos CC obrigatórios (*mandatory*) ou de recomendação (*guidance*), referentes a aplicações de SmartCards.

Tab.10 - Documentos do CC referentes a SmartCards.

5.1.1.1 Normas CC referentes a *smart cards*

Normas	Título	Classe
2006-06-001	*Rationale for Smart cards and similar devices*	
CCDB-2010-03-001	*Guidance for smartcard evaluation v2.0*	*Guidance*
CCDB-2014-04-001	*Security Architecture requirements (ADV_ARC) for smart cards and similar devices*	*Mandatory*
CCDB-2009-03-002	*Application of CC to Integrated Circuits v3.0*	*Mandatory*
CCDB-2012-04-001	*Composite product evaluation for Smartcards and similar devices v1.2*	*Mandatory*
CCDB-2007-09-02	*ETR-template lite for composition v1.0*	*Guidance*
CCDB-2012-04-003	*Security Architecture requirements (ADV_ARC) for smart cards and similar devices*	*Mandatory*
CCDB-2012-04-004	*Security Architecture requirements (ADV_ARC) for smart cards and similar devices - Appendix 1*	*Guidance*
CCDB-2013-05-001	*Requirements to perform Integrated Circuit Evaluations*	*Mandatory*
CCDB-2013-05-002	*Application of Attack Potential to Smartcards*	*Guidance*
CCMB – 2012-09-001	*Part 1: Introduction and general model*	*Mandatory*
CCMB – 2012-09-002	*Part 2: Security functional components*	*Mandatory*
CCMB – 2012-09-003	*Part 3: Security assurance components*	*Mandatory*
CCMB-2012-09-004	*Evaluation methodology*	*Mandatory*

Protection Profiles para ICs, smart Cards e dispositivos/ sistemas relacionados

Na Tab. 11, são apresentados alguns dos PP´s mais relevantes para sistemas de Smart Cards, relacionados tanto ao chip, quanto a *applets*, sistema operacional e leitoras [17]. Os PP´s listados são referentes a aplicações comuns mas não restritas a eID.

Tab.11 - Protection Profiles para sistemas de Smart Cards [17]

Assur-ance Level	Protection Profile	Ano	País	Assurance Family
EAL1+	**Intersector Electronic Purse and Purchase Device (Version for Pilot Schemes), Version 1.2**	1999	França	
EAL3+	**Protection Profile Standard Reader - Smart Card Reader with PIN-Pad supporting eID based on Extended Access Control**	2014	Alemanha	ADV_FSP.4 ADV_IMP.1 ADV_TDS.3 ALC_TAT.1 AVA_VAN.3
	Secure Smartcard Reader with Human Interface	2011	França	ADV_FSP.4 ADV_IMP.1 ADV_TDS.3 ALC_FLR.3 ALC_TAT.1 AVA_VAN.3
	Common Criteria Protection Profile electronic Health Card Terminal (eHCT), Version 1.73	2007	Alemanha	
EAL4	**Machine Readable Travel Document with ICAO Application Extended Access Control with PACE, Version 1.3**	2012	Alemanha	ALC_DVS.2 ATE_DPT.2 AVA_VAN.5
EAL4+	**Personal Number Cards Protection Profile**	2014	Japão	ALC_DVS.2 AVA_VAN.5
	Protection Profile for the Security Module of a Smart Metering System	2013	Alemanha	AVA_VAN.5
	Card Operating System Generation 2	2013	Alemanha	ALC_DVS.2 ATE_DPT.2 AVA_VAN.5
	Java Card System Protection Profile - Closed Configuration version 3.0	2013	França	ALC_DVS.2 AVA_VAN.5
	Java Card System Protection Profile - Closed Configuration version 2.6	2010	França	ALC_DVS.2 AVA_VAN.5
	Java Card™ System Protection Profile Open Configuration, Version 3.0	2012	França	ALC_DVS.2 AVA_VAN.5
	Java Card™ System Protection Profile Open Configuration, Version 2.6	2010	França	ALC_DVS.2 AVA_VAN.5

	JavaCard System Standard 2.2 Configuration Protection Profile, Version 1.0b	2003	França	ADV_IMP.2 AVA_VLA.3
	PP SUN Java Card System Protection Profile Collection	2003	França	ADV_IMP.2 AVA_VLA.3
	ePassport Protection Profile V2.1, Version 2.1	2010	Coreia do Sul	ADV_IMP.2 AVA_VAN.4
	ePassport Protection Profile V2.0, Version 2.	2010	Coreia do Sul	AVA_VAN.4 AVA_VLA.4
	ePassport Protection Profile V1.0	2008	Coreia do Sul	
	Protection Profile for ePassport IC with Active Authentication, Version 1.0	2010	Japão	ALC_DVS.2 AVA_VAN.5
	Electronic Residence Permit Card (RP_Card PP), Compliant to EU - Residence Permit Specification, Version 1.0	2010	Alemanha	ALC_DVS.2 ATE_DPT.2 AVA_VAN.5
	Security Module Card Type B (PP-SMC-B), Version 1.2	2009	Alemanha	
	Security Module Card Type A (PP-SMC-A), Version 1.2	2009	Alemanha	
	Electronic Identity Card (ID_Card PP), Version 1.03	2009	Alemanha	ALC_DVS.2 ATE_DPT.2 AVA_VAN.5
	PP Embedded Software for Smart Secure Devices Basic and Extended Configurations, Version 1.0	2009	França	
	Health Professional Card (PP-HPC) with SSCD Functionality, Version 1.10	2009	Alemanha	AVA_VAN.5
	Protection Profile for electronic Health Card (eHC) - elektronische Gesundheitskarte (eGK)	2010	Alemanha	AVA_VAN.5
	UK Dual-Interface Authentication Card, Version 1.0	2009	Reino Unido	ALC_DVS.2 AVA_VAN.5
	JICSAP ver2.0 Protection Profile part2, Protection Profile for Smart Cards with the Application Program Loading Function (version 1.7e), Version 1.7e	2003	França	
	BAROC CC 3.1 Smart Card Protection Profile, Version 1.0	2007	Alemanha	

	Protection Profile for Contact and Contact free Electronic Wallet, Version 1.2	1999	França	
	JICSAP ver2.0 Protection Profile part1, Multi-Application Secure System LSI Chip Protection Profile, Version 2.5	2003	França	
	Intersector Electronic Purse and Purchase Device (version without last purchase cancellation), Version 1.3	2001	França	
	Intersector Electronic Purse and Purchase Device, Version 1.2	1999	França	
	Automatic Cash Dispensers / Teller, Version 1.0	1999	França	AVA_VLA.3
	Transactional Smartcard reader, Version 2.0	2000	França	
	Smartcard embedded software, Version 1.2	1999	França	
	Smart Card Security User Group - Smart Card Protection Profile (SCSUG-SCPP), Version 3.0	2001	França	
	Smart Card Security User Group - Smart Card Protection Profile, Version 3.0	2001	Canada	
	Machine Readable Travel Document SAC (PACE V2) Supplemental Access Control, Version 1.0	2010	França	ALC_DVS.2 AVA_VAN.5
	Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP)	2011	Alemanha	ATE_DPT.2 AVA_VAN.5
	Protection Profile for Machine Readable Travel Document with 'ICAO Application', Basic Access Control, Version 1.10	2009	Alemanha	ALC_DVS.2
	Resident Registration Card V2 Embedded Software Protection Profile, Version 1.0	2011	Japão	AVA_VAN.5
	(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations, Version 2.0.2	2010	França	ALC_DVS.2 AVA_VAN.5
	(U)SIM Java Card Platform Protection Profile / Basic Configuration (ref. PU-	2010	França	ALC_DVS.2

	2009-RT-79, version 2.0.2), Version 2.0.2			
	Smart Card Open Platform Protection Profile V2.1	2010	Coreia do Sul	AVA_VAN.4
	ELECTRONIC IDENTITY CARD ACCESS DEVICE FIRMWARE PROTECTION PROFILE	2012	Turquia	ALC_DVS.2

- Circuitos Integrados (CI´s) utilizados em Smart Cards

Na Tab. 12, são extraídos da çlista acima alguns dos PP´s mais relevantes para os Circuitos Integrados (CI´s) utilizados em sistemas de Smart Cards com aplicação genérica.

Tab.12 - Protection Profiles para CI´s em Smart Cards

Assurance Level	Protection Profile	Ano	País	Assurance Family
EAL4+	**Security IC Platform Protection Profile with Augmentation Packages** **BSI-CC-PP-0084**	2014	Alemanha	ALC_DVS.2 AVA_VAN.5
EAL4+	**Security IC Platform Protection Profile, Version 1.0** **BSI-PP-0035**	2007	Alemanha	
	Smart Card IC Platform BSI-PP-0002	2001	Alemanha	
EAL4+	**Smart Card IC with Multi-Application Secure Platform, Version 2.0** **FCB PP/0010**	2001	França	
EAL4+	**Smartcard Integrated Circuit Protection Profile, Version 2.0**	1999	França	ADV_IMP.2 ALC_DVS.2 AVA_VLA.4
EAL4+	**Smart Card Integrated Circuit with Embedded Software, Version 2.0**	1999	França	ADV_IMP.2 ALC_DVS.2 AVA_VLA.4

O Protection Profile (PP) mais popular para CI´s de segurança aplicados em Smart-Card é o: *Security IC Platform Protection Profile Version 1.0,* conhecido como CC-PP-0035-2007. Este Protection Profile é estabelecido pelo Eurosmart e pela indústria de Circuitos Integrados e Smartcards, e representa uma atualização do PP *Smartcard IC*

Platform Protection Profilte CC-PP-0002-2001.18. Ambos os smartcards com contato e sem contato usam este protection profile [15].

A Tab.13 faz uma breve descrição dos TOE´s, o número de registro e dos níveis EAL (e as famílias correspondentes) dos principais PP para ICs, Smart Cards e dispositivos /sistemas relacionados. Vale notar que a maioria dos Chips de mercado utilizados atualmente para eID cards, e descritos anteriormente nas tabelas da Seção 3, utilizam estes *Protection Profiles* listados nas tabelas 8 e 9 como referência de certificação.

Tab.13 - Descrição do TOE e no nível EAL dos principais Protection Profiles para ICs, Smart Cards e dispositivos / sistemas relacionados

Título PP	Número de registro	Assurance Level	TOE
Standard Reader - Smart Card Reader with PIN-Pad supporting eID based on Extended Access Control	BSI-CC-PP-0083 29/11/2013	EAL3 ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1 AVA_VAN.3	- Leitora SmartCard com PIN-Pad de acordo com o padrão STANDARD da norma BSI TR-03119, suportando o protocolo EAC e as funções da eID alemã. O objetivo do TOE é realizar a parte do terminal referente ao PACE conforme norma TR-03110 e oferecer gerência de PIN com uma inserção segura.
Smartcard Integrated Circuit Protection Profile	V2.0, issue September 1998	EAL 4 ADV_IMP.2 ALC_DVS.2 AVA_VLA.4	- O intuito deste PP é de especificar requisitos funcionais e de avaliação aplicáveis a IC´s de smartcards baseados em microcontroladores e com interface de comunicação (com ou sem contato ou com ambas)
Security IC Platform Protection Profile, Version 1.0	V1.0 23/08/2007	EAL 4+ ALC_DVS.2, AVA_VAN.5.	PP proposto por Atmel, Infineon Technologies AG, NXP Semiconductors, Renesas Technology Europe Ltd., e STMicroelectronics. O TOE é um IC de segurança com CP, componentes de segurança e portas I/O (com ou sem contato, USB,MMC) e memórias voláteis ou não-voláteis. O TOE pode ainda incluir software dedicado (*firmware)*, e hardware de teste.
Electronic Identity Card (ID_Card PP),	BSI-CC-PP-0061 Version 1.03 16/12/2009	EAL4+ ALC_DVS.2 ATE_DPT.2 AVA_VAN.5	- O TOE desta PP é uma eID (ID_Card) com interface sem contato, conforme a norma BSI TR-03110, version 2.02, com as aplicações ePassport, eID e eSign. O TOE deve cobrir o hardware do chip, todos os softwares dedicados, o Sistema operacional e as aplicações ePassport, eID e, opcionalmente eSign; além da documentação de referência.
Smartcard Integrated Circuit Protection Profile,	Version 2.0 PP/9806	EAL4+ ADV_IMP.2 ALC_DVS.2 AVA_VLA.4	- Este PP foi conduzido pelo "French IT Security Evaluation and Certification Scheme" e proposto por Motorola Semiconductors, Philips Semiconductors, Siemens Semiconductors, STMicroelectronics, Texas-Instruments Semiconductors. O

	01/04/1999		TOE é composto de CPU, elementos de segurança, portas I/O e memórias volátil e não-volátil. O TOE inclui quaisquer softwares dedicados necessários para teste. O software dedicado pode ser firmware ou programas relevantes de segurança ao IC. O TOE pode incluir dados de pré-personalização.

Na Tabela 14, são apresentados alguns modelos de Chips para eID com o seu PP correspondente. Considerando que os recursos de segurança evoluem com o tempo, é necessária a pesquisa por padrões de proteção (PP) da Common Criteria mais recentes. Uma forma eficiente de pesquisa é a consulta de PP`s especificados nos chips voltados para eIDs lançados recentemente.

Tab.14 - Protection Profiles para alguns CI´s comerciais para eID.

Empresa	Produto	Certificação	Protection Profile	Registro
NXP	SmartMX	CC EAL5+ EMVCo	*Eurosmart Smartcard IC Platform Protection Profile Version 1.0, July 2001*	BSI-PP-0002
Infineon	Família SLE78	CC EAL6+ EMVCo	*Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP)* *Machine Readable Travel Document with „ICAO Application", Basic Access Control* *Eurosmart Smartcard IC Platform Protec-tion Profile Version 1.0, July 2001*	BSICC-PP 56v2 (EAC, SAC) BSI-CC-PP 55 (BAC) BSI-PP-0002
Infineon	SLE 66CLX1600PE (M/S)	CC EAL5+	*Eurosmart Smartcard IC Platform Protection Profile Version 1.0, July 2001*	BSI-PP-0002
Infineon	Família SLE88	CC EAL5+ EMVCo	*Eurosmart Smartcard IC Platform Protection Profile Version 1.0, July 2001*	BSI-PP-0002

5.2 Federal Information Processing Standard (FIPS 140-2)

Federal Information Processing Standard (FIPS 140-2) [9] é um padrão de segurança utilizado para validar módulos criptográficos em computadores e sistemas de comunicação. O Instituto americano NIST (*National Institute of Standards and Technology*) publicou o FIPS afim de definir os requisitos e normas para os módulos de criptografia, com foco no hardware e no software. Em termos gerais, esta norma especifica os requisitos de segurança que serão atendidos por um módulo criptográfico [5]. Além disso, este padrão é usado pelo ITI (Instituto de Tecnologia da Informação) nos requisitos de homologação de hardware criptográfico no âmbito da ICP Brasil. A certificação FIPS140-2 certificação / avaliação aplica-se apenas ao módulo criptográfico e não permite uma abordagem global sobre as várias peças que compõem o módulo (como hardware / IC , sistema operacional, e applet) . Estas certificações são concedidas de acordo com o Programa de Validação de módulo criptográfico (Cryptographic Module Validation Program - CMVP), um programa americano/canadense de segurança para avaliar e certificar módulos criptográficos. Todos os testes no âmbito do CMVP são tratados por laboratórios terceirizados que são credenciados como laboratórios de ensaio de módulos criptográficos por parte do Programa Nacional de Reconhecimento de Laboratórios Voluntários (National Voluntary Laboratory Accreditation Program - NVLAP) [15].

Além do padrão FIPS 140-2 ser utilizado para validar módulos criptográficos em software, alguns produtos comerciais já apresentam soluções em hardware que atendem aos requisitos de segurança do FIPS 140-2, como por exemplo os discos rígidos (HD) seguros.

O módulo criptográfico deve empregar mecanismos de segurança física no chip a fim de restringir o acesso físico não autorizado ao conteúdo do módulo. A documentação deve descrever os mecanismos de segurança física aplicáveis que são utilizado pelo módulo . Os conteúdos do módulo, incluindo todo o hardware, firmware, software e dados devem ser protegidos. Todos os hardware, software e componentes de firmware do módulo criptográfico deve ser identificado na documentação do fornecedor. Componentes a serem listados devem incluir: Circuitos integrados, incluindo

processadores, memória e (semi-) circuitos integrados personalizado; outros elementos de circuito eletrônico ativos; entradas e saídas de energia e fontes de alimentação internas ou conversores; estruturas físicas, incluindo placas de circuito e conectores; módulos de software e firmware entre outros.

Além disso, o módulo deve ser fabricado com uma qualidade padrão de produção de CI, projetado para atender um nível comercial das especificações para potência, temperatura, confiabilidade, choques e vibrações, etc. Após a fabricação, o módulo deve usar uma técnica padrão de passivação (passivation techniques) para o chip inteiro. Por fim, o módulo deve apresentar tecnologias clássicas de Circuitos Integrados (Standard Integrated Circuits) e material exterior (encapsulamento) uniforme e conectores padronizados [26].

O padrão FIPS 140-3 (Draft) [9] é um padrão de segurança de computador usado para credenciar os módulos criptográficos . O título deste padrão é *Security Requirements for Cryptographic Modules*. A publicação estava prevista para assinatura pelo Secretário do Comércio, em agosto de 2013, no entanto, ainda está em projeto e não foi oficialmente emitida . O FIPS 140-3 (Draft) é a proposta de revisão do FIPS 140-2, após a descoberta de uma importante falha de segurança na tolerância algorítmica criptográfica do FIPS 140-2 [9].

5.2.1 Requisitos de Segurança para módulos criptográficos

Os requisitos de segurança descrevem 11 áreas relacionadas com a concepção e implementação de um módulo criptográfico, conforme apresentado na Tabela 11. Para cada área, um módulo criptográfico recebe uma classificação de nível de segurança (1-4), dependendo dos requisitos de segurança. Uma avaliação geral é emitida para o módulo criptográfico, que indica [9]:

- o mínimo das avaliações independentes recebidos nas áreas com níveis;

- o cumprimento de todas as exigências nas outras áreas;

No certificado de validação de um fornecedor, as classificações individuais estão listadas, bem como a classificação geral. É importante salientar que, dependendo do ambiente em que o módulo criptográfico seja implementado, a avaliação de uma área específica pode ser mais importante do que a classificação geral.

Tab.15 - Sumário dos requisitos de segurança. Fonte [9].

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Níveis de segurança

O padrão FIPS 140-2 define quatro níveis de segurança. Porém, este padrão não especifica em detalhes o nível de segurança que é exigido por qualquer aplicação em particular:

Nível 1: fornece o menor nível de segurança. Neste nível, requisitos de segurança básicos são especificados, porém, não há mecanismos de segurança física específicos.

Nível 2: aprimora os mecanismos de segurança física de um módulo criptográfico através de controle ao acesso físico, como por exemplo, selos e revestimentos invioláveis.

Nível 3: capacidade de detectar e responder às tentativas de acesso físico, uso ou modificação do módulo criptográfico.

Nível 4: fornece o mais alto nível de segurança. Neste nível de segurança, os mecanismos de segurança física fornecem uma solução completa de proteção em torno do módulo criptográfico com a intenção de detectar e responder a todas as tentativas não autorizadas de acesso físico.

5.2.2 Normas Internacionais

Algumas normas internacionais referentes ao padrão FIPS-140 foram publicadas:

- *ISO/IEC 19790 Tecnologia da Informação - Técnicas de segurança - Requisitos de segurança para módulos criptográficos* (2ª edição 2012). Esta norma foi derivada do FIPS 140-2 PUB, "Requisitos de segurança para módulos criptográficos".

- *ISO/IEC 24759 Tecnologia da Informação - Técnicas de segurança - Requisitos de teste para módulos criptográficos* (2a edição 2014). Esta norma foi derivada do FIPS 140-2 PUB, "Requisitos de Teste NIST derivados para FIPS PUB 140-2, Requisitos de segurança para módulos criptográficos".

5.3 Certificados para cartões EMVCo

Os certificados EMVCo[11] são utilizados para verificar a interoperabilidade a nível mundial de operações de pagamento seguras através das especificações definidas pela EMV (Europay, MasterCard, Visa). Atualmente as especificações da EMV estão baseadas em chips de contato, chips sem contato, pedidos de pagamento comum (*common payment application* - CPA), cartões de personalização e Tokens.

Esta certificação é atualmente supervisionada por seis organizações: American Express, Discover, JCB, MasterCard, UnionPay e Visa.

O Grupo de Trabalho de Avaliação de Segurança (Security Evaluation Working Group - SEWG é responsável por avaliar a segurança de todas as implementações do aplicativo de pagamento comum EMVCo (Common Payment Application - CPA). O objetivo principal do processo de avaliação de segurança EMVCo é garantir que os CI´s e cartões inteligentes CPA´s estejam em conformidade com as diretrizes de segurança EMVCo. A avaliação de segurança IC inclui as rotinas de firmware e software necessários para acessar as funções do CI de segurança. A avaliação da segurança do cartão inteligente CPA inclui o CI, o sistema operacional e todos os aplicativos de pagamento comuns que estão inseridos no cartão inteligente. A Secretaria de Avaliação EMVCo Segurança é responsável pela administração do processo de avaliação de segurança EMVCo. De comum acordo, a MasterCard Worldwide executa as funções da Secretaria de Avaliação EMVCo de segurança, utilizando os recursos do Laboratório de Análises MasterCard (MCAL). A metodologia utilizada no processo de avaliação utiliza um programa de pesquisa destinado ao procedimento de ataque.

O processo de avaliação de segurança EMVCo foi concebido para fornecer um "alto" nível de garantia , tal como definido no pedido de documento de ataque potencial em Smartcards para produtos de cartões inteligentes, CI´s e CPA, em todas as fases do desenvolvimento. Além das avaliações de segurança EMVCo para cartões EMV de crédito e cartões de débito, as diferentes marcas internacionais de pagamento (American Express, Discover , JCB, MasterCard e Visa) tem avaliações de segurança específicas para os seus pedidos de pagamento exclusivos para os cartões de tarja magnética e smart cards [15].

As marcas de pagamento individuais (American Express , Discover , JCB , MasterCard , Visa) ainda mantém a responsabilidade pela avaliação da segurança de seus aplicativos de pagamento individuais , independentemente destas aplicações serem com chips com contato ou sem contato [15].

Na certificação EMVCo, os produtos com chips (CI´s) são avaliados e aprovados com uma data de vencimento (*expiry date*), em conformidade com as regras de renovação da associação da EMVCo e respeitando as regras de segurança pré-estabelecidas. Vale

salientar que o prazo máximo de validade de um certificado EMVCo para um determinado produto (chip) é de 6 anos. Conforme [11], a Tab.16 apresenta os chips, com as respectivas empresas fornecedoras, para os quais o EMVCo aprovou e emitiu um Certificado de Conformidade. A análise destes padrões é relevante para a análise dos requisitos de segurança para uma eventual emissão de cartões EMV com *applet* eID.

Tab.16: Certificados para CI´s aplicados a EMVCo em 2015 [11].

Infineon Technologies AG				
ICCN	**Produto**	**Versão**	**Emissão**	**Expiração**
ICCN0142	M7820	A11	31 Oct 2009	31 Oct 2015
ICCN0144	M7820	(DCLB) A11	31 Oct 2009	31 Oct 2015
ICCN0146	M7790	A12	03 Dec 2010	03 Dec 2015
ICCN0155	M7820	M11	21 Apr 2011	21 Apr 2015
ICCN0160	M7793	A12 / G12	08 Jul 2011	08 Jul 2015
ICCN0161	M7794	A12 / G12	20 Dec 2011	20 Dec 2015
ICCN0163	M7892	A21 / B11	11 Jan 2012	11 Jan 2016
ICCN0178	IFX_ECI_7h:[1h-56h]	-	22 Jun 2012	22 Jun 2015
ICCN0193	M7791	B12	08 Aug 2013	08 Aug 2015
ICCN0200	M7893	B11	20 Dec 2013	20 Dec 2015
ICCN0209	IFX_ECI_15h [1h-11h]	-	22 Jun 2012	22 Jun 2015
INSIDE Secure				
ICCN	**Produto**	**Versão**	**Emissão**	**Expiração**
ICCN0147	AT90SC9604RV	Rev. I	24 Feb 2011	24 Feb 2015
ICCN0157	AT90SC20818RCV	Rev: C / C1	28 Jun 2011	28 Jun 2015
ICCN0159	AT90SC13608RCV	Rev. E	27 Jul 2011	27 Jul 2015
ICCN0164	AT90SC28880RCV	Rev. B	13 Feb 2012	13 Feb 2015
ICCN0173	AT90SC20818RCFV	Rev. F	01 Jun 2012	01 Jun 2015
ICCN0175	AT90SC352208RCV	Rev. C	13 Sep 2012	13 Sep 2015
ICCN0192	AT90SC28880RCFV2	Rev. C	31 May 2013	31 May 2015
NXP Semiconductors Gmbh				
ICCN	**Produto**	**Versão**	**Emissão**	**Expiração**
ICCN0128	P5CD081	V1A / V1A(s)	30 Sep 2009	30 Sep 2015

ICCN0149	P5CD145V0A/V0B & V0B(s)	V0A / V0B & V0B(s)	16 Mar 2011	16 Mar 2016
ICCN0150	P5CC012	V1A & V1A(s)	26 Apr 2011	26 Apr 2015
ICCN0166	P5CD081	V1D	30 Sep 2009	30 Sep 2015
ICCN0169	P60D024PVB(Y/Z/A)/PVF, P60D024MVB(Y/Z/A)/yVF y=M,D	VB, VF	01 Jun 2012	01 Jun 2015
ICCN0170	P60D144PVA/PVA(Y/B)PVE, P60D144yVA/yVA(B)/yVE; y=M,D,J	VA, VE	16 May 2012	16 May 2015
ICCN0183	P60x080/052/040PVC(Y/Z/A)/PVG &P60D080/052/040yVC(Z/A)/yVG	VC(Y) / VC(Z)/VG	10 Jan 2013	10 Jan 2016
ICCN0195	P61N1M3P	VD	20 Oct 2013	20 Oct 2015
ICCN0197	P60D041PVD	VD	30 Sep 2013	30 Sep 2015
ICCN0201	P40C072VA V0.9 / P40C072VD V1.1	VA, VD	14 Feb 2014	14 Feb 2016
ICCN0203	P61N1M3P	VD-1 / VE-1	20 Oct 2013	20 Oct 2015
ICCN0205	P40C072VD	VD	14 Feb 2014	14 Feb 2016
ICCN0207	P60D041PVE	VE	30 Sep 2013	30 Sep 2015
Samsung Electronics Co., Ltd.				
ICCN	**Produto**	**Versão**	**Emissão**	**Expiração**
ICCN0143	S3CT9KW	Rev.2	05 Jul 2010	05 Jul 2015
ICCN0154	S3CT9KA	Rev. 0 / 1	17 May 2011	17 May 2015
ICCN0156	S3CT9PC	Rev. 1	06 Jun 2011	06 Jun 2015
ICCN0162	S3CT9AC	Rev. 0	06 Jun 2011	06 Jun 2015
ICCN0168	S3FV9QM	Rev. 3, 4 and 5	04 May 2012	04 May 2015
ICCN0171	S3CT9P3	Rev. 0	14 Jun 2012	14 Jun 2015
ICCN0181	S3FT9FD	Rev. 1	03 Dec 2012	03 Dec 2015
ICCN0184	S3FT9PF	Rev. 0	29 Mar 2013	29 Mar 2015
ICCN0187	S3FT9PE	Rev. 0	29 Mar 2013	29 Mar 2015
ICCN0190	S3FV9QJ	Rev. 0	13 Jun 2013	13 Jun 2015
ICCN0191	S3FT9MD	Rev. 0/1	29 Jul 2013	29 Jul 2015
ICCN0199	S3FT9MF	Rev. 0 and 1	19 Dec 2013	19 Dec 2015
ICCN0204	S3FT9FA	Rev. 0	30 Apr 2014	30 Apr 2015
ICCN0206	S3FV5RP	0	11 Jul 2014	11 Jul 2015
STMicroelectronics SAS				

ICCN	Produto	Versão	Emissão	Expiração
ICCN0125	ST23YR18	Rev. A	28 Aug 2009	28 Aug 2015
ICCN0126	SB23YR18	Rev. A	28 Aug 2009	28 Aug 2015
ICCN0132	ST/SC33F1M	Rev. E / F	22 Oct 2009	22 Oct 2015
ICCN0133	ST23ZL48	Rev. A (internal D / G)	18 Dec 2009	18 Dec 2015
ICCN0134	SA23ZL48	Rev. A (internal D / G)	18 Dec 2009	18 Dec 2015
ICCN0135	SB23ZL48	Rev. A (internal D / G)	18 Dec 2009	18 Dec 2015
ICCN0167	ST/SC/SP/SM/SE/SL33F1M	Rev. E / F	22 Oct 2009	22 Oct 2015
ICCN0174	ST23ZR08	Rev. A	18 Jul 2012	18 Jul 2015
ICCN0179	ST23YR160	Rev. B(internal rev B/C/D/E)	14 Dec 2011	14 Dec 2015
ICCN0186	SB23Z012	Rev. A (Internal rev. B & C)	15 Apr 2013	15 Apr 2015
ICCN0188	SC23Z018	Rev. A (internal revisi-ons C & H)	15 Apr 2013	15 Apr 2015
ICCN0189	ST31-K330A	Rev. E / F / H / I	30 Apr 2013	30 Apr 2015
ICCN0202	ST33G1M2	Rev. F	14 Feb 2014	14 Feb 2016
Toshiba Corporation				
ICCN	**Produto**	**Versão**	**Emissão**	**Expiração**
ICCN0196	T6ND7	v4.00	01 Oct 2013	01 Oct 2015

6 CONCLUSÃO

Neste relatório foram descritas as características relevantes dos *chips* implementados nos sistemas eletrônicos e nos *smartcards* aplicados em uma solução de eID. Adicionalmente, alguns *chips* comerciais atualmente desenvolvidos e empregados na indústria foram apresentados. Ademais, foram apontados alguns exemplos de eID nacionais, com as características gerais dos respectivos *chips* utilizados. Além disso, foram descritas as certificações e normas empregadas neste tipo de aplicação, bem como uma análise detalhada dos termos e definições utilizadas nos certificados de segurança.

Com base nos estudos técnicos e na comparação dos *chips* disponíveis no mercado, podemos descrever algumas características mínimas necessárias para a especificação de um *chip* de eID. No entanto, para uma recomendação sugerida do *chip* para um eID deverá ser levado em conta a capacidade de armazenamento de dados do *chip*, a segurança dos dados, o atendimento aos critérios das certificações e padrões e as aplicações inseridas do sistema de identificação.

Algumas características são essenciais para definirmos o *chip* adequado a uma determinada aplicação e seus recursos, como: interface de comunicação, processador lógico (CPU), tipos e tamanhos das memórias, coprocessador criptográfico, gerador de números aleatórios (RNG) e unidade de gerenciamento de memória (MMU). Abaixo, serão detalhadas as especificações recomendadas.

- O *chip* deverá ser capaz de armazenar as informações e configurações mínimas do sistema e das aplicações, das chaves e assinaturas/certificados digitais e possuir um coprocessador capaz de realizar operações criptográficas apropriadas.
- Os *chips* com microprocessadores utilizados em *smartcards* são específicos para cada aplicação, ou seja, não são utilizados os processadores "padrões" largamente utilizados pela indústria eletrônica de consumo. Os motivos desta especificidade do microprocessador são: custo de fabricação, funcionalidade (coprocessador criptográfico, segurança) e área do silício (*chip*) limitada pelo cartão.
- O chip deverá ser programável e multi-aplicativo. Ou seja, capaz de carregar novas aplicações e excluir as informações e aplicações desnecessárias, sendo assim, possível de se adaptar e sofrer alterações de uso ao longo do tempo.

- O tamanho mínimo da memória depende das aplicações do sistema. No entanto, o *chip* deverá ser capaz de armazenar as informações confidencias mínimas e funcionalidades requeridas do sistema de processamento e de criptografia. Além disso, o *chip* deve possuir memórias não-voláteis do tipo EEPROM/FLASH (armazenamento seguro de informações) e ROM (armazena permanentemente, durante a fabricação do *chip*, algumas instruções do Sistema Operacional), bem como memórias voláteis do tipo RAM (memória operacional, que armazena variáveis e resultados intermediários da CPU e dados de entrada/saída).
- Uma durabilidade atual aceitável para o armazenamento das informações e confiabilidade do funcionamento do sistema é de no mínimo 10 anos.
- O *chip* deverá possuir um sistema de proteção da memória (MMU) contra ataques externos, definição de senhas de acesso aos arquivos restritos e condições de acesso diferenciadas, de acordo com os diferentes usuários. Adicionalmente, este sistema de proteção deve restringir o acesso externo de determinadas informações, por exemplo, chaves privadas armazenadas.
- Interface de comunicação de dados para o leitor externo com-contato *(Contact),* definida pela norma ISO/IEC 7816-3, *ou sem-contato (Contactless)*, definida pela norma ISO/IEC 14443.
- Possuir um coprocessador de criptografia que implemente em *hardware* diversas operações criptográficas, permitindo uma alta eficiência nos cálculos matemáticos, necessários para as funções de criptografia. Este coprocessador deve suportar os algoritmos de criptografia simétricos, como o DES (3-DES) e o AES, ou os assimétricos, como o RSA e curvas-elípticas.
  - O *chip* deve apresentar um gerador de números aleatórios genuínos (implementado em *Hardware*), ao invés de um gerador pseudoaleatório (comumente implementado por *Software*).
  - Ser certificado com a certificação do *Common Criteria* (CC), no mínimo, no nível de avaliação de segurança EAL 4+. O EAL4 permite que um desenvolvedor obtenha uma garantia máxima de segurança com base nas boas práticas de desenvolvimento comerciais e é, em geral, o nível mais alto para que seja economicamente viável a certificação de uma linha de produtos existente. Os outros níveis, EAL5, EAL6 e EAL7

apresentam um nível se segurança mais elevado. Porém, possuem custos excessivos atribuíveis a técnicas especializadas de engenharia de segurança.

- Atender os requisitos do padrão FIPS 140-2 para o módulo criptográfico (*Hardware* e *Software*). O padrão FIPS 140-2 define quatro níveis de segurança. Porém, este padrão não especifica em detalhes o nível de segurança que é exigido por qualquer aplicação em particular.

Por fim, existem diversas alternativas para os *chips* utilizados em *smartcard* e em identidades eletrônicas. Neste estudo, procurou-se abordar os principais aspectos relacionados aos *chips* empregados em um documento de identificação eletrônica. No entanto, vale ressaltar que existe um constante avanço no desenvolvimento de novas tecnologias de circuitos integrados. Deste modo, torna-se necessário um acompanhamento contínuo dos avanços do estado da arte desta tecnologia e das soluções atuais disponíveis no mercado afim de se definir um sistema adequado de identidade eletrônica nacional que atenda todas as especificações elétricas e de segurança.

7 REFERÊNCIAS BIBLIOGRÁFICAS

[1] W. Fumy and M. Paeschke, *Handbook of eID Security: Concepts, Practical Experiences, Technologies,* Wiley, ISBN: 978-3-89578-379-1, Jan. 2011.

[2] W. Rankl and W. Effing, *Smart Card Handbook*, 4a Edição, Wiley, 2010.

[3] http://www.iso.org/iso/home.htm

[4] http://www.commoncriteriaportal.org/

[5] K. Konechy, Designing for FIPS 140-2 and Common Criteria Compliance, Valicore Technologies Inc., for Networksystemsdesignline.com, Nov., 2005

[6]http://www.infineon.com/

[7] http://www.digikey.com/product-search/en/integrated-circuits-ics

[8] http://www.chipfind.net/datasheet/comm/smartcard/1.htm

[9] National Institute of Standards and Technology (NIST), *Federal Information Processing Standards, FIPS 140-2, Security Requirements for Cryptographic Modules,* May 2001

[10] http://www.seagate.com.br

[11] http://www.emvco.com

[12] Common Criteria for Information Technology Security Evaluation, *Part 1: Introduction and general model*, website http://www.commoncriteriaportal.org, version 3.1, revision 4, 2012.

[13] Nuevo Documento de Identidad, GEMALTO, 2015.

[14] Notification Award, Bangladesh Election Commission IDEA Project, 2014

[15] Smart Card Alliance, *What Makes a Smart Card Secure?* , A Smart Card Alliance Contactless and Mobile Payments Council White Paper, www.smartcardalliance.org, 2008.

[16] Laackmann P. and Janke M., *Reducing risks for government ID security chips*, The Vault, Krowne Communications GmbH, Germany, no. 9, 2011.

[17] http://www.commoncriteriaportal.org/pp_IC.html#IC

[18] D. d. Cock, Katholieke Universit Leuven, 2005 "http://homes.esat.kuleuven.be/~decockd/slides/2005.11.24.belgian.eid.card.technical.overview.for.ipa.herfstdagen.the.netherlands.pdf,".

[19] S. Arora, "Review and Analysis od Current and Future European e-ID Card Schemes," Eoyall Holloway University od London, 2007.

[20] D3.6 Study on ID Documents," Future of Identity in the Information Society, 2006.

[21] http://eid.belgium.be/nl/binaries/RN406_tcm227-238941.pdf

[22] Aguado, Jose Luiz Diez, DNI 3.0 Seguridad Informatica y Communicaciones, Regional Seminar on MRTDs and Traveller Identification Management, 2014, Madrid, Espanha

[23] G. H. Ingo Naumann, "Privacy Features of European eID Card Specifications," ENISA (Europena Network and Information Security Agency, 2009.

[24] "Study on eID Interoperability for PEGS: Update of Country Profiles," IADBC European Comission, 2009.

[25] A. Lehmann, "Survey and Analysis of Existing eID and Credential Systems," Future Id Project, Abril 2013.

[26] NIST, CSEC and CMVP Laboratories, Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules,* Jan., 2011

Universidade de Brasília – UnB

Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

www.unb.br – www.cdt.unb.br – www.latitude.eng.br