UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO E PROPOSTA DE UM NOVO DOCUMENTO DE IDENTIFICAÇÃO ELETRÔNICA (e-ID) PARA O BRASIL

YAMAR AIRES DA SILVA

ORIENTADOR: RICARDO STACIARINI PUTTINI

DISSERTAÇÃO DE MESTRADO
EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: 296/2007

BRASÍLIA / DF: FEVEREIRO/2007

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO E PROPOSTA DE UM NOVO DOCUMENTO DE IDENTIFICAÇÃO ELETRÔNICA (e-ID) PARA O BRASIL

YAMAR AIRES DA SILVA

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

Ricardo Staciarini Puttini, Doutor, UnB
(ORIENTADOR)

Rafael Timóteo de Sousa Jr., Doutor, UnB
(EXAMINADOR INTERNO)

Mamede Lima-Marques, Doutor, UnB
(EXAMINADOR EXTERNO)

Anderson Clayton Nascimento, Doutor, UnB
(SUPLENTE)

DATA: BRASÍLIA/DF, 28 DE FEVEREIRO DE 2007.

FICHA CATALOGRÁFICA

DA SILVA, Yamar Aires
Estudo e Proposta de Um Novo Documento de Identificação Eletrônica (e-ID) para o Brasil [Distrito Federal] 2007.
xx, 167 p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2007).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. e-ID 2. Documento de Identificação
3. Cartão Inteligente

I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

DA SILVA, Y. A. (2007). Estudo e Proposta de Um Novo Documento de Identificação Eletrônica (e-ID) para o Brasil. Dissertação de Mestrado, Publicação 296/2007, Departamento de Engenharia Elétrica, Universidade de Brasília , Brasília , DF, 167p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Yamar Aires da Silva
TÍTULO DA DISSERTAÇÃO: Estudo e Proposta de Um Novo Documento de Identificação Eletrônica (e-ID) para o Brasil.
GRAU/ANO: Mestre/2007.

Yamar Aires da Silva
SQN 309 Bloco A Apto. 104
CEP 70755-010 – Brasília – DF - Brasil

Dedicatória

Dedico este trabalho à minha família e aos meus amigos. Aos meus pais e meus irmãos pelo eterno apoio, à minha esposa por todo seu amor e carinho e ao Rafa, o gorducho simpático.

Dedico aos Amigos pela constante confiança e camaradagem.

AGRADECIMENTOS

Ao meu orientador e Amigo Doc, Prof. Dr. Ricardo Staciarini Puttini, pela contribuição imprescindível no desenvolvimento do tema e das minhas habilidades como pesquisador.

Ao Prof Dr. Rafael Timóteo de Sousa Júnior, pela disponibilização de conteúdos e discussões proveitosas.

A todos que colaboraram, os meus sinceros agradecimentos.

RESUMO

Esta dissertação tem como objetivo o estudo e a análise dos conceitos, processos e tecnologias envolvidos na produção de documentos de identificação eletrônica e a proposta de um novo documento de identificação para o Brasil, levando-se em consideração as necessidades brasileiras e as aplicações desejadas para este documento. O estudo proposto nessa dissertação avalia as alternativas tecnológicas para os componentes envolvidos na confecção de documentos de identificação eletrônica, no que diz respeito à mídia de suporte, considerando-se o uso de cartões inteligentes, e aos requisitos de segurança de documentos de identificação civil. É feita ainda uma análise da legislação em vigor no Brasil, com objetivo de identificar as informações que devem constar no novo modelo de Cartão Nacional de Identificação de acordo com as premissas da Lei 9.454, de 07 de abril de 1997. Existem diversas alternativas tecnológicas e possibilidades de uso de um documento de identificação eletrônica. Este trabalho procura abordar os principais aspectos relacionados à tecnologia de documentos e tem como contribuição mais saliente a proposição de elementos técnicos para composição de um documento de identificação alinhados com as possibilidades de uso desse documento.

ABSTRACT

This thesis objectives a conceptual, processual and technological analisys involved in the production of electronic identification documents (e-ID). It also objectives a proposal for a new e-ID for Brazil, given respect the Brazilian needs and desired applications. It evaluates the technological elements regarding the production of an e-ID, from card materials to secuity features.A legislation analisys from Brazilian federal law N. 9.454, regarding the information a new Brazilian e-ID card should present is also considered. Tehere are many technological alternatives and possibilities that should be considered in order to produce an e-ID. Therefore, this thesis wishes to approach the main aspects related to document issuing iniciatives, in order to proposal technical elements for producing e-ID's according to the possibilities and the targets once reqired for such a task.

ÍNDICE

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

LISTA DE ACRÔNIMOS

ABS – Acrylonitrile butadiene styrene

APDU – Application Protocol Data Unit

CC – Common Criteria

CSE – Canadian Security Establishment

EEPROM – Electrically Erasable Programmable Read-Only Memory

GSC-IS – Government Smart Card Interoperability Specification

ICAO – International Civil Aviation Organization

IEC – International Electrotechnical Commision

ISO – International Organization for Standardization

MRTD – Machine Readable Travel Documents

NICSS – Next generation IC Card System Study

NIST – National Institute of Standards and Technology

NVM – Nonvolatile Memory

OCR – Optcal Character Recognition

OSCIE – Open Smart Card Infrastructure for Europe

PC – Policarboneto

PET – Poli Tereftalato de Etila

PVC – Policloreto de Vinila

RAM – Random Access Memory

ROM – Read-Only Memory

1. INTRODUÇÃO

Os documentos de identificação eletrônica (e-ID) surgiram através dos cartões de bancos, com o objetivo de prover maior segurança nas transações financeiras. Comumente, são cartões plásticos embutidos com vários itens de segurança tais como tecnologias de impressão de segurança, tarjas magnéticas, códigos de barras e mais tarde com a adição de chips, quando surgiram os cartões inteligentes (smart cards).

Inicialmente, procurou-se transferir as tecnologias de impressão segura usadas na confecção de papel moeda para os cartões plásticos. A maioria dessas tecnologias é aderente à fabricação de documentos seguros em cartões plásticos. Porém, o novo meio, o plástico, abriu um grande leque de alternativas para novas tecnologias de segurança, não só na impressão segura bem como na própria fabricação e customização dos cartões.

A utilização de tarjas magnéticas, códigos de barras e chips tem por objetivo implementar transações eletrônicas seguras, onde os documentos são lidos e autenticados por máquinas oferecendo uma gama de serviços e aplicações. Como exemplo mais comum podemos citar o caixa eletrônico dos bancos.

Desde então, a utilização de cartões plásticos vem ganhando aplicações diversas na sociedade em geral. A identificação funcional dentro de empresas e órgãos públicos, o acesso a clubes, associações e até academias de ginástica já são implementados, de uma forma ou de outra, com documentos de identificação eletrônica.

Portanto, é natural que governos e suas autoridades caminhem na direção de adotar documentos de identificação civil, como carteira de motorista, título de eleitor e passaporte, mais modernos e seguros. A constante tensão criada por ameaças terroristas, tráfico de drogas e contrabandos reforça ainda mais esta necessidade.

Muitos países já começaram ou tem a iniciativa de adotar cartões inteligentes na confecção de documentos de identificação civil. A Figura 1-1 ilustra o status de desenvolvimento de projeto de e-ID na Europa. Outras regiões do globo também possuem iniciativas no sentido de estabelecer programas de identificação civil usando o conceito de e-ID.

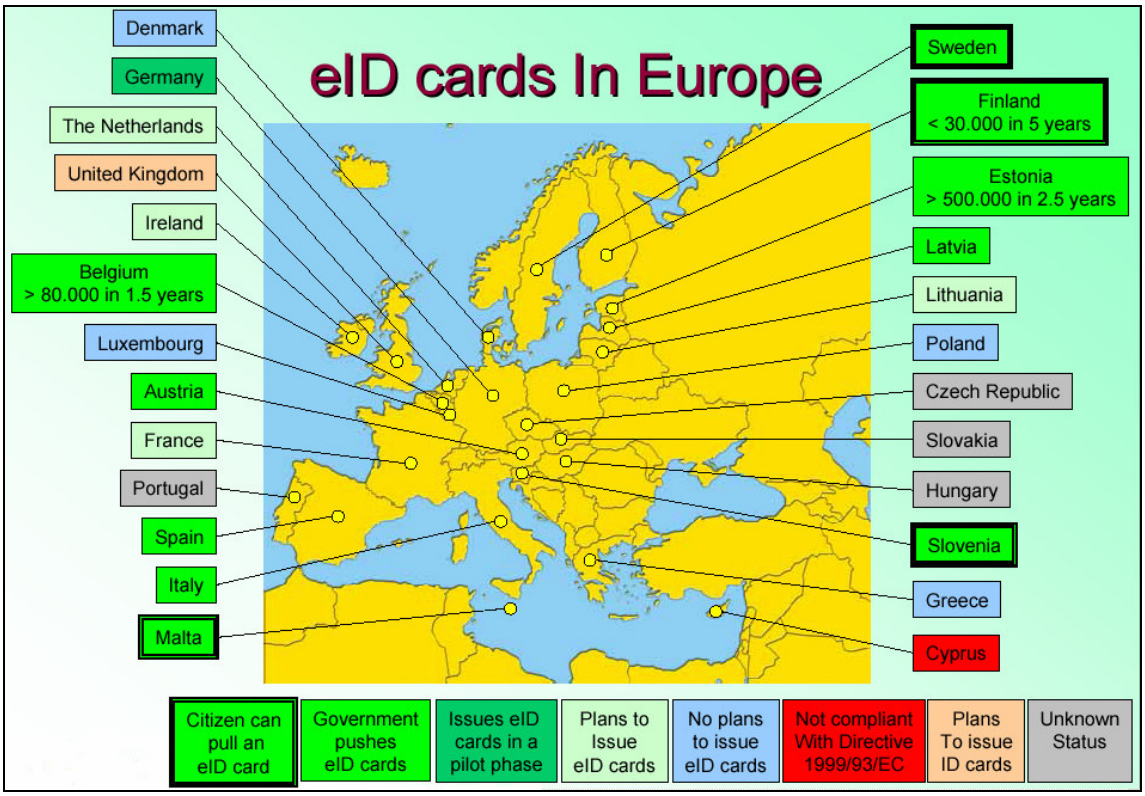


Figura 1-1 – Panamora sobre e-ID na Europa
Fonte: http://www.esat.kuleuven.ac.be/cosic

1.1. NORMAS INTERNACIONAIS

Um grande número de normas e padrões vem sendo desenvolvido em muitas partes do globo. Esta seção apresenta inicialmente uma contextualização das iniciativas mundiais para a concepção de projetos de identificação de cidadãos com uso de cartões inteligentes (e-ID) e de biometria.

A ICAO (International Civil Aviation Organization) trabalha na padronização de documentos desde 1968 em uma divisão de Cartões Passaporte. Esta divisão ficou encarregada de desenvolver recomendações para padronização de livros de passaporte ou cartões que pudessem ser lidos mecanicamente com o intuito de acelerar o tramite de passageiros nos controles de fronteira.

Esta divisão produziu um grande número de recomendações, dentre elas, a adoção de um padrão de leitura ótica de caracteres (OCR) para leitura mecânica com baixo custo e alta confiabilidade. Em 1980, estas recomendações foram publicadas na primeira edição do

documento Doc 9303 - A “Passport with Machine Readable Capability”, que se tornou base para emissão de documentos de viagem para Austrália, Canadá e Estados Unidos.

Em 1997, a TAG/MRTD (Technical Advisory Group on Machine Readable Travel Documents) lançou a primeira edição revisada da Doc 9303, dividida em três partes, sendo a primeira destinada a livros de passaporte, a segunda para vistos consulares e a terceira para cartões.

Em 2002, foi lançada a secunda edição da Doc 9303 [28]. Esta edição foi e revisada em maio de 2003. Vale frisar que a Doc 9303 partes 1, 2 e 3 é endossada pela ISO (International Organization for Standardization) como ISO 7501-1, 7501-2 e 7501-3 respectivamente. Outras normas e especificações internacionais são mostrados na Tabela 1-1.

Tabela 1-1 – Normas Internacionais

Referência	**Descrição**
[EUR-Lex]	**Resolution of the representatives of the governments of the Member States,** reunião do Conselho de 17 de Outobro 2000 suplementando resoluções de 23 junho 1981, 30 junho 1982, 14 de julho 1986 e 10 de julho 1995 em relação a características de segurança de passaportes e outros documentos de viagem (Official Journal C 310, 28/10/2000 p. 0001)
ICAO 9303 Part 3: 2002	**Machine Readable Travel Documents -** Size 1 and Size 2 Machine Readable Official Travel Documents
ISO 1073-2: 1976	**Alphanumeric character sets for optical character recognition –** Part 2: Character set OCR-B – Shapes and dimensions of the printed image
ISO 1831: 1980	**Printing specifications for optical character recognition**
ISO 3166-1: 1997	**Codes for the representation of names of countries and their subdivisions –** Part 1: Country codes
ISO 8601: 2001	**Data elements and interchange formats -** Information interchange – Representation of dates and times
ISO/IEC 7501-3:1997	**Machine Readable Travel Documents –** Identity Cards
ISO/IEC 7810: 1995	**Identification cards –** Physical characteristics
ISO/IEC 7812-1: 2000	**Identification cards –** Identification of issuers **–** Numbering system
ISO/IEC 10646-1	**Character set Unicode**
[ITRSS]	**Security Standards for Machine Readable Travel Documents**, Technical report, ICAO
SS 614314	**Identification card – Identity card of type ID-1**, (Identifieringskort –Identitetskort av typ ID-1)

O uso da biometria com impressões digitais vem se destacando no cenário de identificação de grandes populações, a exemplo do processo de identificação civil na Coréia do Sul e no sistema de controle de imigração dos EUA. Este também é o sistema escolhido para integrar o novo passaporte digital europeu e a carteira de identificação civil digital (e-ID) em países como a França e a Alemanha [18].

Muitos projetos de e-ID estão combinando o uso de biometria com smart cards para aumentar a segurança e a privacidade dos sistemas de identificação.

Em um relatório técnico recente, a ICAO apresenta um apanhado do estado da arte da tecnologia de biometria para aplicações em controle de identidade a ser incorporado em documentos de viagem (passaporte) lisíveis por máquina (MRTD – Machine Readable Travel Documents). Esse documento, que vem sendo usado como referência em projetos de e-passaporte e de e-ID, apresenta alguns cuidados importantes a serem observados quando do uso de técnicas de biometria para identificação de grandes populações:

- As técnicas de biometria usadas por diversos fornecedores encontram-se em desenvolvimento rápido e contínuo;
- A grande maioria dos produtos/soluções não foi testada por um período longo (10 anos ou mais);
- Não há provas de uso de sistemas biométricos para identificação (1:N) em bases de dados grandes com populações de uma mesma nação;
- Dadas as rápidas mudanças do estado da tecnologia, qualquer especificação deve permitir, e reconhecer que sofrerá, modificações resultantes de melhorias tecnológicas.

A Biometric Application Program Interface (BioAPI), desenvolvida pelo BioAPI Consortium (http://www.bioapi.org/), provê um modelo genérico de autenticação biométrica de alto nível com objetivo de prover interoperabilidade entre diversas aplicações que utilizam tecnologia de biometria. A BioAPI v1.1 se tornou um padrão ANSI (ANSI INCITS 358-2002) em fevereiro de 2002 [4].

1.2. E-ID NO BRASIL

A identidade civil, no Brasil, apresenta inúmeros problemas de conceito, arquitetura e segurança. O fato da identificação civil ser prerrogativa dos estados é um grande problema, pois o cadastro é descentralizado e portanto o número de identificação não é único, tornando possível a um cidadão brasileiro possuir um documento de identidade em cada estado, diferente do cadastro de CPF, onde um único número é gerado pela Receita Federal para cada cidadão.

A segurança do documento é frágil. Impresso em papel moeda com poucos itens de segurança, a identidade brasileira é quase um convite a fraudes. Apesar da impressão digital contida no documento ser um item bastante seguro, é de difícil autenticação, pois normalmente exige a inspeção de um profissional, o papiloscopista, para validar a autenticidade do portador do documento.

Por fim, os processos envolvidos na emissão do documento são pouco seguros. O fluxo do papel moeda utilizado na confecção do documento, apesar de controlado, não é auditável. O descarte, inutilização, estravio, entre outros, fazem parte da rotina de processos frágeis que levam em consideração a arquitetura descentralizada e autônoma dos estados.

Uma iniciativa importante é a normalização e lançamento do e-CFP, realizado pela Receita Federal em 2005, sendo este talvez o único caso de documento emitido em larga escala por entidades de governo e com a finalidade de identificação de cidadãos que se enquadre no conceito de e-ID.

1.3. ESTUDO DE ALTERNATIVAS

Esta dissertação tem como objetivo o estudo e a análise dos conceitos, processos e tecnologias envolvidos na produção de documentos de identificação eletrônica e a proposta de um novo documento de identificação para o Brasil, levando-se em consideração as necessidades brasileiras e as aplicações desejadas para este documento. O estudo proposto nessa dissertação avalia as alternativas tecnológicas para os componentes envolvidos na confecção de documentos de identificação eletrônica, no que diz respeito à mídia de suporte, considerando-se o uso de cartões inteligentes, e aos requisitos de segurança de documentos de identificação civil.

É feita ainda uma análise da legislação em vigor no Brasil, com objetivo de identificar as informações que devem constar no novo modelo de Cartão Nacional de Identificação de acordo com as premissas da Lei 9.454, de 07 de abril de 1997. Apresentam-se ainda os vários fatores que serão considerados na definição para o novo modelo da cédula nacional de identificação, dentre os principais pode-se citar:

- Identificação Visual do Cartão - definição das informações a serem impressas no cartão, tais como, dados pessoais, dados dos cadastros civil e eleitoral e fotografia, entre outros, incluindo o layout padronizado do cartão;

- Armazenamento Digital de Informações no Cartão - definição das informações a serem armazenadas digitalmente no cartão, tais como, dados pessoais , dados do cadastro civil e eleitoral, fotografia, pseudônimo, impressões digitais, entre outros, incluindo a definição de quais informações poderão ser lidas por máquina a partir do cartão;

- Tipo de material: definição do tipo de material a ser usado na confecção do cartão.

- Requisitos de Segurança - uso combinado de mecanismos de assinatura e certificação digital com diversas técnicas de segurança de cartões plásticos digitais que possibilitam dificultar ou mesmo evitar a reprodução fraudulenta de cartões, tais como: técnicas especiais de impressão, inserção de dispositivos ópticos (e.g. holografia) e utilização de cartões com chip embutido (smart card).

1.4. ORGANIZAÇÃO DO TRABALHO

O restante desta dissertação está organizado da seguinte maneira: No Capítulo 2 é apresentada uma revisão da tecnologia de cartões inteligentes. O capítulo 3 discute os aspectos relacionados com a fabricação de cartões plásticos usados em documentos de identificação. O Capítulo 4 descreve os principais mecanismos de segurança para documentos emitidos em cartões plásticos. O Capítulo 5 apresenta um conjunto de premissas de uso e as respectivas opções tecnológicas para a definição de um novo documento de identificação eletrônica (e-ID) para o Brasil. Finalmente, o Capítulo 6 apresenta as conclusões deste trabalho.

2. CARTÕES INTELIGENTES (SMART CARDS)

Os primeiros cartões de crédito de plástico surgiram da necessidade de se substituir o dinheiro por um meio de pagamento mais seguro. Porém, a garantia que se tinha era apenas a assinatura do portador do cartão, que deveria ser idêntica à marcada no verso desse mesmo cartão. Dessa maneira, tarjas magnéticas foram incorporadas aos cartões. Essas tarjas armazenavam informações digitais que podiam ser lidas por maquinas especificamente projetadas para esse fim. Porém, os dados armazenados nas tarjas magnéticas podem ser facilmente lidos, apagados ou sobrescritos por pessoas com acesso ao equipamento necessário. Dessa forma, o sistema não é indicado para armazenamento de informações confidenciais. Tornaram-se necessárias novas técnicas que garantissem a confidencialidade dos dados e a prevenção da manipulação dessas informações.

O advento dos smart cards, combinados à expansão de sistemas de processamento de dados eletrônicos, trouxe uma série de novas possibilidades para o desenvolvimento de muitas soluções. As primeiras soluções de integração de circuitos lógicos com dispositivos de armazenamentos surgiram na Alemanha e na França, em meados dos anos 70. Os primeiros dispositivos a utilizar tecnologia semelhante aos atuais smart cards foram os cartões telefônicos desenvolvidos nesses mesmos países, nos anos 80. O crescimento de pesquisas na área da criptografia também foi muito importante para consolidação dos smart cards, principalmente em aplicações bancárias, que exigem um alto grau de segurança. Em 1984, um banco francês começou a aplicar esse tipo de tecnologia nas suas transações.

Um smart card é um cartão, de tamanho semelhante a um cartão de crédito, que contém um ou mais circuitos integrados (CIs), e que pode ainda empregar uma das seguintes tecnologias de armazenamento de dados: tarja magnética, código de barras (linear ou bidimensional), transmissores sem fio (que utilizam radio freqüências), além de informações biométricas, criptografia e autenticação ou identificação por foto. O circuito integrado contido no cartão pode atuar como um microcontrolador ou como um computador. Dados podem ser armazenados na memória do chip e podem ser acessados por múltiplas aplicações. Além disso, na memória do chip existe um sistema operacional, programas de comunicação (transferências de dados), podendo ainda conter algoritmos de criptografia para manter os dados e aplicações ilegíveis para quem não possuir a chave do algoritmo.

Quando utilizado em conjunto com aplicações adequadas, esses cartões podem gravar, armazenar e atualizar dados de maneira segura. E, se bem implementados, podem prover a interoperabilidade entre serviços, habilitando o usuário a utilizar múltiplas aplicações com um único cartão.

O chip é o principal componente de um smart card e é a parte do cartão que o difere de um simples cartão com tarja magnética, por exemplo, tornando-o um cartão inteligente.

A combinação da tecnologia de smart cards com aplicações web, comércio eletrônico e outros tipos de negócios na Internet, pode melhorar a qualidade de vida dos cidadãos em geral, ou de empregados de uma empresa, por exemplo. Muitas aplicações podem ser potencializadas com a utilização dos smart cards, dentre as quais pode-se citar:

- Ferramentas de controle de acesso: a segurança que pode ser implementada em um smart card habilita o mesmo a operar como um token de autenticação, para acesso lógico seguro a terminais e redes (LANs ou a própria Internet), bem como para acesso físico a edifícios, estacionamentos, salas ou áreas específicas de uma empresa.

- Ferramentas de pagamento: Os smart cards podem servir como um cartão de crédito, débito, ou seja, podem funcionar como um cartão bancário comum.

- Armazenamento de Informação e Ferramentas de Gerenciamento: dependendo da capacidade de armazenamento do chip, os cartões podem armazenar e gerenciar dados auxiliares para várias aplicações. Por exemplo, informações médicas armazenadas no smart card poderão ser acessadas por pessoal autorizado, em uma ocasião de emergência ou em uma visita médica de rotina. As informações presentes no cartão poderão diminuir substancialmente o tempo gasto com a recuperação de informações armazenadas em papel.

- Capacidade de Acesso Seguro: o uso de tecnologias sofisticadas, como a biometria, aumenta de maneira notável a segurança na verificação de identidade, para acesso lógico ou físico. Podem ser utilizadas chaves públicas ou privadas para assinaturas digitais e criptografia de e-mails, por exemplo. A utilização de recursos biométricos e de chaves públicas ou privadas em conjunto podem trazer grande acurácia na identificação de um indivíduo.

2.1. CLASSIFICAÇÃO

De acordo com Rankl e Effing [58], os smart cards podem ser classificados quanto ao tipo do chip (chip de memória ou com microcontrolador) e quanto ao método de transmissão de dados (com contato, sem contato ou de dupla interface). Os chips de memória são ainda divididos nos que possuem e nos que não possuem lógica de segurança. Os autores ainda subdividem os chips com microcontroladores nos que possuem ou não possuem co-processador. A Figura 2-1 ilustra essa classificação.

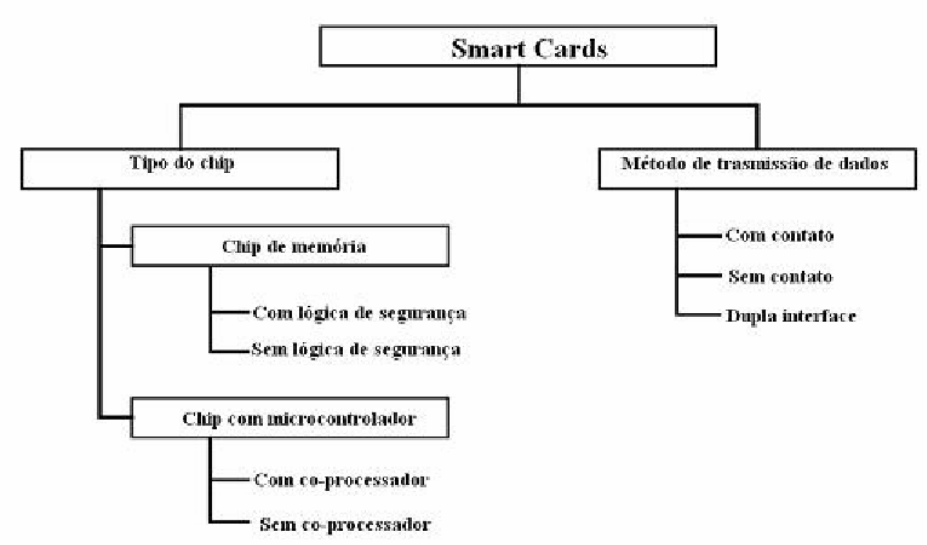


Figura 2-1 – Classificação de Smart cards

Fonte: adaptado de Rankl & Effing [58]

Quanto à inteligência (tipo do chip), os smart cards podem ser apenas de armazenamento de dados (chip de memória) ou podem possuir uma unidade de processamento de informações (microcontrolador):

- Chip de Memória: os dados necessários à aplicação são armazenados na memória, que geralmente é uma EEPROM (Electrically Erasable Programmable Read-Only Memory). O acesso à memória é controlado por uma lógica de segurança, que, no caso mais simples, consiste apenas em uma proteção contra escrita ou apagamento de dados de regiões da memória. Alguns chips possuem lógica de segurança mais complexa, que podem até prover encriptação simples. Cartões de memória

possuem aplicação restrita (cartões telefônicos pré-pagos e armazenamento de dados médicos), porém o custo é muito baixo.

- Chips com microprocessadores: o elemento central do chip é um processador. Esses tipos de cartões podem ser usados por aplicações variadas. Os smart cards mais modernos possuem alta capacidade de processamento e grande capacidade de armazenamento de dados.

Existem dois tipos principais de interface dos cartões - de contato ou sem contato. Esses termos referem-se à maneira com que a energia é fornecida ao chip e com que os dados são transferidos do chip para um dispositivo de leitura. Alguns cartões utilizam dois chips separados (dupla interface). Esses cartões são conhecidos como cartões híbridos, de dupla interface ou combi.

Um smart card sem contato do tipo mais usado necessita de uma proximidade de aproximadamente 10 centímetros da leitora para transferência de dados. A transferência é realizada através de ondas de rádio freqüência (RF). Existe uma antena interna ao cartão, que facilita a comunicação entre o chip e a leitora.

2.2. CARACTERÍSTICAS FÍSICAS

O formato mais familiar de smart cards é o padrão ID-1 (85,6 mm por 54 mm), que foi especificado pela norma ISO 7810, em 1985, para ser usado em cartões de identificação. Essa norma definia apenas um cartão de plástico com uma tarja magnética. A presença de um chip e a localização de contatos no cartão só foram definidas muitos anos depois em outros padrões. Os cartões utilizados em terminais telefônicos móveis GSM, são do formato ID-000 (25,10 mm por 15,10mm).

2.2.1. Plástico

O primeiro material empregado nos cartões de identificação foi o PVC (Policloreto de Vinila). O PVC é o material mais barato entre os disponíveis, é fácil de processar e apropriado a uma grande quantidade de aplicações. É utilizado no mundo todo em cartões de crédito. Porém, existem muitas desvantagens do uso do PVC, o que vem tornando sua utilização cada vez mais limitada nos últimos anos. Entre essas desvantagens, destaca-se o fato de o cloreto

de vinila ser um conhecido agente cancerígeno e que hidrocloretos e dioxinas[1] são compostos químicos resultantes da queima do PVC. Além disso, metais pesados são utilizados como estabilizadores na produção de PVC. Graças a essas questões, muitos fabricantes de cartão têm decidido não utilizar o PVC, por políticas de proteção do ambiente.

Em substituição ao PVC, o ABS (do inglês Acrylonitrile Butadiene Styrene, ou co-polímero de acrilonitrila, butadieno e estireno) tem sido utilizado por algum tempo na produção de cartões. É mais tolerante a altas temperaturas que o PVC e é utilizado, graças a essa característica, na produção de smart cards para telefones móveis.

Para aplicações em que se exige grande estabilidade e durabilidade, o PC (policar-boneto) é uma opção. É tipicamente utilizado em cartões de identificação e é base para materiais utilizados na produção de CDs e DVDs. Possuem alto custo quando comparado aos demais materiais.

Um material que não agride a natureza é o PET (Poli Tereftalato de Etila), já que pode ser reprocessado e reutilizado diversas vezes, e vem sendo utilizado como substituto ao PVC na fabricação de smart cards. Pode ser utilizado em sua forma amorfa (A-PET) ou cristalina (PETP).

Muitas pesquisas têm buscado encontrar materiais melhores para o corpo dos smart cards (como o acetato de celulose e o próprio papel), porém nenhum deles ainda foi utilizado em grandes escalas.

Uma discussão mais detalhada acerca do material utilizado para fabricação de cartões pláticos, evidenciando as características físicas que devem ser ressaltadas no seu uso em documentos de identificação é apresentada no capítulo 3.

2.2.2. CHIP

A principal característica que distingue os tipos de smart cards é o chip de Circuito Integrado (CI) presente nesse cartão, além da forma de contato físico entre o cartão e a leitora. Os primeiros smart cards foram cartões de memória, contendo um CI apenas com memória não-volátil e o circuito necessário para leitura e escrita nessa memória.

[1] Um dos compostos químicos mais tóxicos que podem ser produzidos pelo homem, podendo ser letais em um simples contato com a pele.

A Figura 2-2 abaixo mostra os contatos de um smart card típico de contato, que é composto por oito conexões elétricas distintas. Os tipos mais comuns de smart cards utilizam dois conectores na face do cartão para atuar como um canal de I/O (entrada e saída) half-duplex para transmissão de dados da leitora para o cartão e vice-versa.

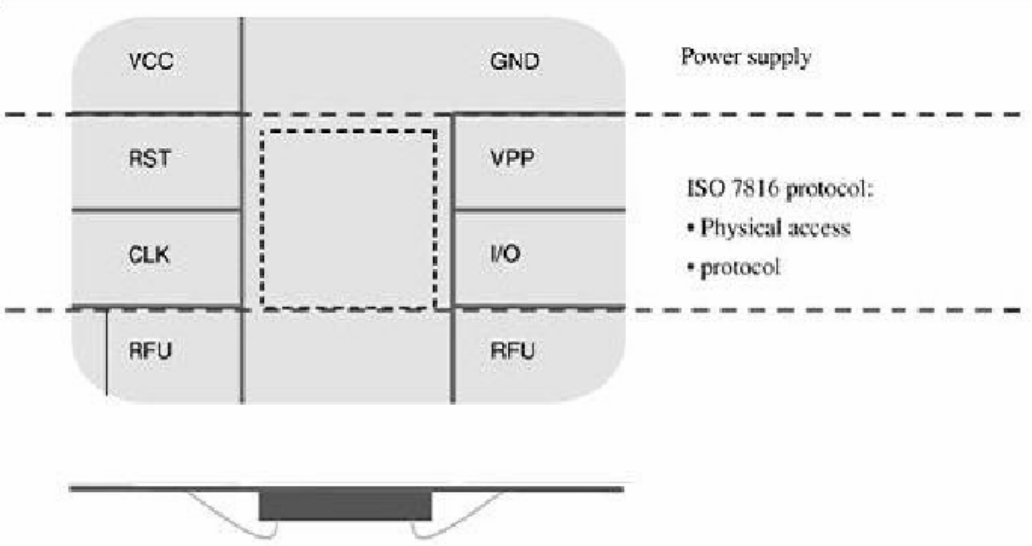


Figura 2-2 - Layout dos contatos de um Smart Card

Fonte: adaptado de Rankl & Effing [58]

De acordo com a ISO 7816, os contatos acima são responsáveis pelas seguintes funções, mostradas na Tabela 2-1.

Tabela 2-1 - Função de cada contato de um Smart Card

Contato	Função
VCC	Provisão de tensão
RST	Reset
CLK	Clock
RFU	Reservados para uso futuro
GND	Terra
VPP	Tensão de programação
I/O	Input/Output para comunicação serial

Fonte: adaptado de Rankl & Effing [58]

2.2.2.1. Processador

A CPU dos smart cards podem ser microcontroladores de 8 a 32 bits, que utilizam conjuntos de instruções para acesso e escrita em memória, manipulações de registradores, modos de endereçamento e operações de I/O. Alguns fabricantes estenderam o conjunto básico de instruções para outras particularmente desenvolvidas para uso em CPUs dos smart cards.

- Interface física: O canal de I/O em um smart card é um canal serial unidirecional. Ou seja, só se pode passar um bit por vez, e os dados podem uir apenas em um sentido por vez. A capacidade de transmissão do smart card é geralmente bem superior àquela suportada pela leitora, isto é, a velocidade de transmissão dos dados será determinada pela capacidade de transmissão/recepção de dados da leitora. O protocolo de comunicação entre o smart card e a leitora é baseado em uma relação de mestre (leitora) e escravo (smart card). A leitora (ou um host conectado a ela) envia solicitações de dados para o smart card e espera por uma resposta. O smart card nunca envia dados sem a solicitação do host.

- Energia: É suprida da leitora para o cartão. A maioria dos smart cards opera entre 3,5V e 5V.

- I/O: Duas interfaces são utilizadas para carregar tráfego I/O entre a leitora e o cartão. Uma linha, a linha de I/O, carrega os bits de dados. Esta linha pode assumir dois estados, 1 ou 0. A segunda linha, o clock, indica quando a linha de I/O deve ser amostrada para determinação do bit de dados.

- Sincronização: Os protocolos típicos que são utilizados para comunicação entre a leitora e o cartão são os protocolos half-duplex. Ou seja, os dados são tanto escritos na linha de I/O pela leitora e lidos pelo cartão quanto escritos pelo cartão e lidos pela leitora. Dessa maneira, cada final da linha de comunicação determina qual dispositivo está em um estado de leitura ou escrita. Como esses protocolos não são muito sofisticados, é possível que ocorram erros que deixem um ou ambos os terminais do canal em um estado ambíguo. Quando isso ocorre, é responsabilidade da leitora resetar toda a seqüência do protocolo. Isso pode ser realizado com o pino reset.

2.2.2.2. Memória

Existem basicamente quatro tipos de memória amplamente utilizadas em smart cards: ROM (Read-Only Memory), EEPROM (Electrically Erasable Programmable Read-Only Memory), NVM (Nonvolatile Memory) e RAM (Random Access Memory).

- ROM: Na memória ROM é onde está armazenado o sistema operacional do smart card. As memórias ROM típicas possuem capacidade de armazenamento entre 8kbytes a 96kbytes. É onde se encontram rotinas como as utilizadas para comunicação e para manutenção do sistema de arquivos presente no cartão, além de rotinas de criptografia e rotinas aritméticas para propósitos especiais. Informações de codificação podem ser colocadas na memória ROM, desde que estas não necessitem ser alteradas. Dessa forma, estas informações são intrínsecas ao cartão.

- EEPROM: É utilizada nos smart cards para todos os dados e programas que necessitem ser modificados ou apagados ao mesmo tempo. Funcionalmente, uma EEPROM corresponde a um HD de um computador pessoal, já que ela retém dados na ausência de energia e os dados podem ser alterados quando necessário. É um tipo de memória não-volátil. Uma célula EEPROM corresponde a um capacitor que pode ser carregado (nível lógico 1) ou descarregado (nível lógico 0).

- NVM: Na memória do tipo NVM é onde são armazenados os dados de variáveis, como números de contas, pontos em programas de fidelidade, ou até saldo em conta corrente. Este tipo de memória pode ser lida ou escrita por aplicações, mas ela não funciona exatamente como uma memória RAM. Ela mantém os dados armazenados, mesmo com a parada no suprimento de energia para o cartão. Os dados armazenados nesse tipo de memória, se não forem sobrescritos, podem durar até 10 anos. Porém, é uma memória lenta (geralmente se necessita de 3 a 10 milisegundos para escrever em uma memória NVM) e pode ocorrer perda de dados (a utilização por mais de 100.000 vezes não é recomendada).

- RAM: A memória RAM não é largamente utilizada pelos smart cards, e, quando os chips possuem esse tipo de memória, o espaço disponível para programação não é grande. Como nesse tipo de memória é necessário suprimento de energia contínuo para ma-nutenção dos dados, operações intermediárias podem ser ali

executadas. Como as operações de leitura e escrita nesse tipo de memória são muito rápidas, torna-se importante sua utilização em smart cards. Operações podem ser ali executadas e os resultados armazenados em memórias NVM.

2.2.2.3. Smart Cards Sem Contato

Cartões sem contato não necessitam de nenhum contato físico entre o smart card e o terminal, para transferência de energia ou de dados. Existem três principais tecnologias em uso atualmente: Tecnologia 125kHz, ISO/IEC 14443 e ISO/IEC 15693.

- Tecnologia 125 kHz: É uma tecnologia passiva, já que o campo RF (radio freqüência) emitido pela lei-tora fornece energia ao cartão. Esta tecnologia não é baseada em nenhum padrão ISO/IEC, mas nos padrões da indústria. Esse padrão da indústria ficou conhecido como "Wiegand", nome do inventor da tecnologia. A leitora para tecnologia 125 kHz emite um campo constante operando a 125 kHz. Companhias distintas podem utilizar freqüências ou modulação diferente no retorno para a leitora. Dessa maneira, um cartão de um fabricante não necessariamente opera com uma leitora de outro fabricante.

- Tecnologias ISO/IEC 14443 e ISO/IEC 15693: Utilizam os padrões de nível de aplicação definidos pela ISO/IEC 7816-4, descritos mais adiante na seção 2.3.1. Ambas resolvem problemas de aplicações específicas, e têm crescido em áreas antes utilizadas por outras tecnologias. Ambas utilizam a freqüência de 13,56MHz. A ISO/IEC 14443 é uma tecnologia sem contato com faixa de operação de aproxima-damente 10 cm. Essa tecnologia foi originalmente utilizada para tíquete eletrônico e e-cash (electronic cash). Dessa maneira, são necessárias pequenas distâncias das leitoras e altas velocidades na transmissão de dados. A tecnologia ISO/IEC 15693 foi desenvolvida para operar a distâncias de aproximadamente 1 metro. São especialmente utilizados em estacionamentos, para evitar que os motoristas tenham que estender os braços para leitura dos dados dos cartões de controle.

A Tabela 2-2 apresenta os dados comparativos entre as três principais tecnologias de smart card sem contato utilizadas atualmente.

Tabela 2-2 – Tecnologias de smart card sem contatos			
Características	1443	15693	125 kHz
Normas	ISO/IEC 14443 ISO/IEC 7810	ISO/IEC 14443 ISO/IEC 7810	-
Frequencia	13,56 MHz	13,56 MHz	125 khZ
Alcance operacional	Até 10 Cm	Até 1m	Até 1m
Tipos de chip suortados	Memória Wired logig microcontrolado	Memória Wired logig	Memória Wired logig
Funções de criptografia eautenticação	MIFARE, DES/3DES, AES, RSA,ECC	DES/3DES	-
Capacidade de memória	64 A 64K bytes	256 e 2K bytes	8 A 256 BYTES
Habilidade Ler/escrever	Ler/escrever	Ler/escrever	Leitura apenas
Taxa de transferência de dados Kb/s	Até 106 (ISO) Até 848 (disponível)	Até 26,6	Até 4
Anticolisão	SIM	SIM	Opcional
Autenticação Cartão-Leitora	Challenge/response	Challenge/response	Password
Cartão Híbrido	SIM	SIM	SIM
Suporte a interface de contato	SIM	NÃO	NÃO

2.3. NORMAS E PADRÕES

Atualmente uma série de padrões internacionais define especificações para implementação de smart cards direcionadas para a indústria e para desenvolvimento de aplicações com o foco nestes dispositivos. Cabe salientar que, para as definições do arcabouço tecnológico utilizado para o desenvolvimento dos requisitos técnicos definidos neste documento, foram provenientes dos estudos técnicos realizados nestes padrões.

Esta seção destina-se a explorar com mais profundidade os padrões e normas orientadores e regulamentadores em todo o mundo. Os padrões de Smart Card detalham as propriedades físicas, caracteríscas de comunicacão, e identificadores de aplicação dos chips e dados. Quase todos os padrões se referem à ISO 7816, partes 1, 2 e 3 como referência básica.

As propriedades das aplicações específicas estão sendo debatidas entre grandes grupos e organizações em todo o mundo, e são propostos diversos padrões. A interoperabilidade entre os sistemas abertos de cartões deve-se dar em diversos níveis:

1. Do cartão em si;

2. Dos terminais de acesso (leitoras);

3. Das redes;

4. Dos sistemas proprietários dos provedores dos cartões.

A interoperabilidade dos sistemas abertos de cartão só será alcançada através da conformidade com os padrões internacionais.

Os padrões ISO (International Organization of Standardization) que contém especificações pertinentes à tecnologia smart card são diversos, como a 7816 (dividido em diversas partes) e as ISO 7810, 7811 e 7813, discutidas nas Seções 2.3.1 e 2.3.2. Elas padronizam o tamanho dos cartões, a qualidade do plástico, o posicionamento dos contatos, as freqüências utilizadas em cartões sem contato entre outros.

Nas seções 2.3.3 e 2.3.4 são discutidas normas e padrões para avaliação da segurança e para criptografia e certificação digital, respectivamente. Essas normas, apesar de não tratarem especificamente de smart cards são referenciadas em especificações e certificações de cartões inteligentes usadas em aplicações com requisitos sérios de segurança da informação e que suportam operações criptográficas.

Na seção seguint seção apresentados outros padrões desenvolvidos e aplicados. Finalmente, na seção 2.3.6 é mostrado o enquadramento do Brasil e suas recomendações técnicas.

2.3.1. ISO/IEC 7816

A ISO 7816 é um padrão internacional relacionado com cartões de identificação eletrônicos, especialmente cartões inteligentes microprocessados, gerenciado pela International Organization for Standardization (ISO) e a International Electrotechnical Commision (IEC). Este padrão é uma extensão da ISO 7810. Este padrão é composto por 15 partes no total.

2.3.1.1. 7816-1 – Características Físicas

Esta parte descreve as características físicas de um cartão com circuito integrado, além de definir as características de um cartão ao ser dobrado ou flexionado. O objetivo é assegurar que os cartões com chips sejam produzidos de forma a garantir a operação sem falhas durante sua vida útil. Conexões entre a superfície dos conectores e os chips devem suportar esforços mecânicos. Esta parte da norma é importante principalmente para fabricantes de cartões.

Taz em seu escopo especificações de resistência mínima do material à:

- Luz ultra-violeta
- Raios X;
- Interferência eletromagnética;
- Eletricidade estática;
- Dissipação de calor; e
- Estresse mecânico.

Também faz menção à localização de uma possível trilha magnética. Os testes de resistência do cartão estão descritos na ISO 10373 (vide Capítulo 3).

2.3.1.2. 7816-2 – Dimensões e Localização de Contatos

Esta parte faz menção à dimensão e localização dos contatos elétricos em um smart card de contato (Figura 2-3 e Figura 2-4).

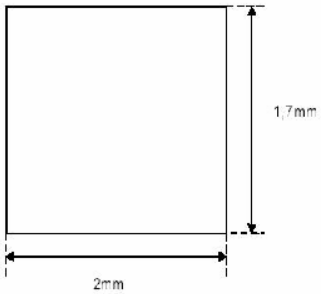


Figura 2-3 - Dimensões mínimas dos contatos elétricos dos cartões inteligentes

Fonte: Manual de Condutas Técnicas [45]

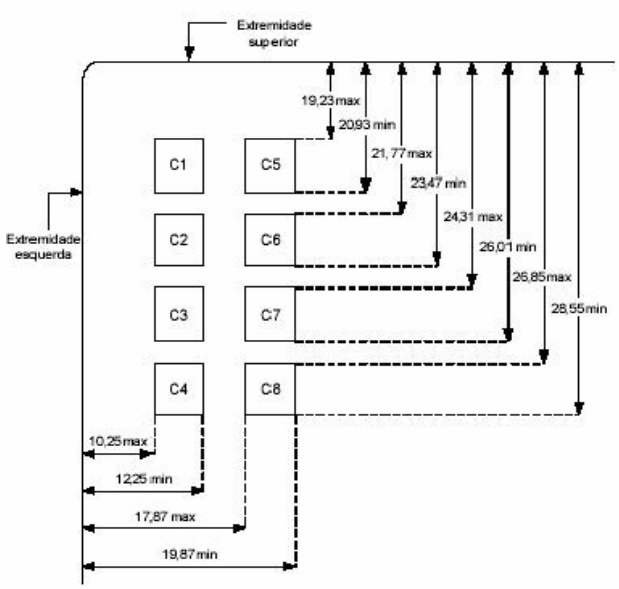


Figura 2-4 - Número e localização dos contatos elétricos dos cartões inteligentes

Fonte: Manual de Condutas Técnicas [45]

Esta parte também cita as funções de cada contato (Tabela 2-1) cabendo ainda afirmar que ela exige que os contatos C4 e C8, reservados para uso futuro, sejam eletricamente isolados do resto do circuito.

2.3.1.3. 7816-3 – Características Elétricas

Descreve sinais eletrônicos e protocolos de transmissão de cartões de circuitos integrados. Esta norma é importante para fabricantes de leitores e desenvolvedores que queiram estabelecer uma comunicação com o cartão inteligente ao nível do sinal eletrônico.

Esta parte descreve os sinais elétricos em cada um dos contatos, como a mínima e máxima voltagem e corrente, define também os procedimentos de operação em cada um dos contatos, além de determinar os protocolos de transmissão (vide Tabela 2-6, mais adiante). Segue, como exemplo, o procedimento do contato RESET (Figura 2-5).

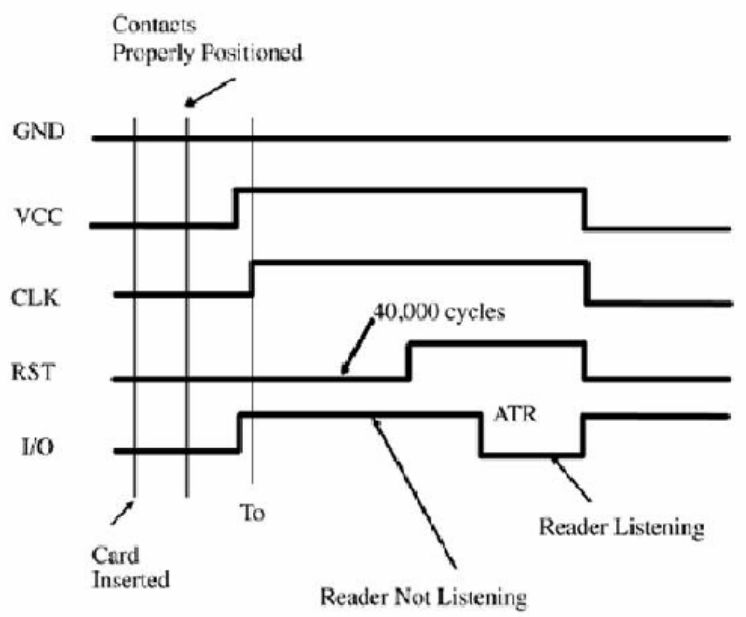


Figura 2-5 - Sequência do procedimento de RESET pela leitora de cartão

Fonte: adaptado de Rankl & Effing [58]

2.3.1.4. 7816-4 – Organização, Segurança e Comandos para Comunicação

Esta é a base para o desenvolvimento dos sistemas operacionais de smart cards. Define os perfis de smart cards, aspectos relacionados a sistemas de arquivos (Seção 2.4.3) e define o conjunto de APDUs. Como exemplo do conteúdo desta parte, aTabela 2-3 mostra o conjunto mínimo de comandos básicos para módulos criptográficos.

Tabela 2-3 - Conjunto mínimo de comandos básicos de interoperabilidade para módulos criptográficos

Comando	Definição e Escopo	Seção ISO 7816-4
READ BINARY	Pode ser usado para ler dados de um EF com estrutura de arquivos transparente, iniciando a leitura de uma posição (*offset*) especificada por um parâmetro passado via comando.	6.1
GET DATA	Utilizado para recuperar ou ler objetos de dados. Tal comando foi especificado para prover acesso direto a objetos de dados.	6.9
PUT DATA	Utilizado para armazenar ou escrebver objetos de dados. Tal comando foi especificado para prover acesso direto a objetos de dados.	6.10
SELECT FILE	Utilizado para selecionar um arquivo (MF, DF ou EF).	6.11
VERIFY	Utilizado para comparar um segredo enviado via interface (PIN, por exemplo) com um valor de referência já armazenado no módulo criptográfico.	6.12

EXTERNAL AUTHENTICATE	Utilizado para autenticar um terminal (leitora) perante um módulo criptográfico.	6.14
GET CHALLENGE	Requer do módulo criptográfico um número randômico para ser usado posteriormente para fins de autenticação.	6.15

Fonte: Manual de Condutas Técnicas [45]

Especifica ainda:

- Conteúdos dos pares de comando-resposta trocados pela interface;
- Meios de leitura dos dados no cartão;
- Estruturas e conteúdos dos bytes históricos para descrever características operativas do cartão;
- Estruturas para aplicações e dados no cartão;
- Métodos de acesso aos arquivos e dados no cartão;
- Uma arquitetura de segurança que define direitos de acesso aos arquivos e dados no cartão;
- Meios e mecanismos para identificar e acionar aplicações no cartão;
- Métodos para envio de mensagens de forma segura;
- Métodos de acesso aos algoritmos processados pelo cartão.

2.3.1.5. 7816-5 – Registro de Provedores de Aplicação

Enquanto a ISO 7816-4 define como usar um identificador da aplicação (AID) para verificar a presença e/ou executar a recuperação de uma aplicação em um cartão, a ISO 7816-5 mostra como conceder a unicidade de identificadores da aplicação com o registo internacional de uma parte deste identificador, e define:

- O procedimento do registro;
- As autoridades encarregadas;

- A disponibilidade do registrador para ligar as partes registradas do identificador e os fornecedores de aplicação relevantes.

O AID é explicado na Seção 2.4.3 e mostrado em detalhe na Figura 2-14.

2.3.1.6. 7816-6 – Elementos de Dados Inter-Indústria para Comunicação

Especifica os elementos de dados (DEs) utilizados para comunicação entre indústrias em cartões de circuito integrado, com contatos e sem contatos. Contém o nome, descrição, formato, codificação e layout de cada elemento de dado e define os meios de leitura dos mesmos.

2.3.1.7. Partes 7 a 15 da ISO 7816

- 7816-7: Comandos para Structured Card Query Language (SCQL).

- 7816-8: Comandos para Operações Seguras. Especifica comandos para cartões de circuito integrado que podem ser usado para operações criptografadas. Estes comandos são complementares e estão baseados nos comandos listados na ISO/IEC 7816-4.

- 7816-9: Comandos para Gerenciamento do Cartão. Especifica comandos para cartões de circuito integrados para gerenciamento de arquivo e cartão, por exemplo, criação e eliminação de arquivos. Estes comandos duram toda a vida útil do cartão e, portanto, alguns comandos podem ser utilizados antes do cartão ser emitido ao usuário ou depois de sua data de vencimento.

- 7816-10: Verificação Pessoal através de Métodos Biométricos. Especifica o uso de comandos e dados relacionados à verificação pessoal através de métodos biométricos em cartões de circuito integrado. Os comandos utilizados estão definidos na ISO/IEC 7814-4. Os dados estão parcialmente definidos nesta norma, parcialmente importados da ISO/IEC 19785-1.

- 7816-12: Cartões com Contatos – Interface USB e Procedimentos de Operação. Especifica as condições de operação de um cartão de circuito integrado que possui uma interface USB, que é chamado de USB-ICC.

- 7816-13: Comandos para Gerenciamento de Aplicações em Ambientes Multi-Aplicação.
- 7816-15: Aplicação para Informação Criptográfica. Especifica uma aplicação do cartão. Esta aplicação contém informação sobre a funcionalidade de criptografia. Além disso, a norma define uma sintaxe e formato para a informação criptográfica e mecanismos para compartilhar a mesma quando apropriado.

2.3.2. Outros padrões ISO diretamente relacionados com smart cards

2.3.2.1. ISO 7810

Esta ISO é responsável pela padronização do formato dos cartões. Temos como principais formatos definidos por esta ISO:

- ID-1, formato tradicional de um cartão de crédito, mostrado na Figura 2-6.
- ID-000, formato tradicional de um SIM card, cartão usado em telefones celulares, mostrado na Figura 2-7.

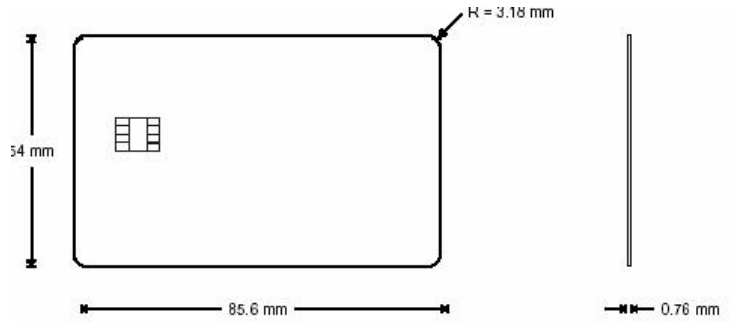


Figura 2-6 - Formato ID-1 e suas medidas

Fonte: adaptado de Rankl & Effing [58]

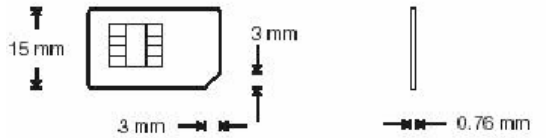


Figura 2-7 - Formato ID-000 e suas medidas

Fonte: adaptado de Rankl & Effing [58]

O padrão 7810 elenca outros formatos, mas não tão difundidos e por isso de pouco interesse para este trabalho.

2.3.2.2. ISO 7811

Este padrão especifica as trilhas magnéticas para cartões com esta opção. Não menciona os cartões inteligentes, mas os smart cards podem oferecer a opção de tarja magnética e, neste caso devem seguir este padrão. A tarja magnética segue pode ter até 3 trilhas (normalmente conhecidas por *tracks*), conforme a Figura 2-8.

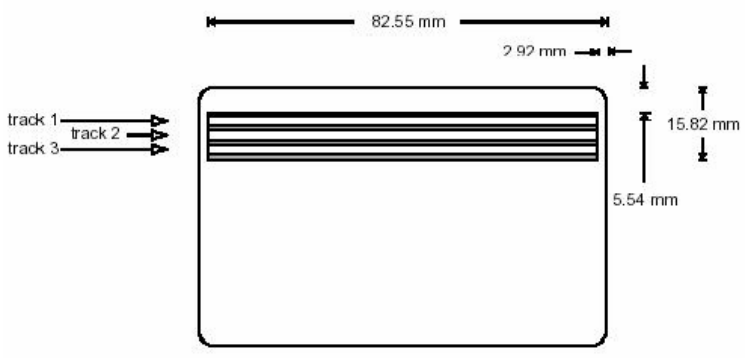


Figura 2-8 - As três trilhas de uma tarja magnética

Fonte: adaptado de Rankl & Effing [58]

2.3.2.3. ISO 7813

É uma continuação da ISO 7810. Define padrões de cartões para operações financeiras. Entre outras coisas esta norma define os cantos arredondados dos cartões de crédito e também o tipo de codificação usada nas tarjas magnéticas.

2.3.2.4. ISO 14443

Cartões de proximidade (contactless) - descreve os padrões para cartões de proximidade. Estabelecem os padrões para características físicas, energia por radio freqüência, freqüência de rádio e sinais elétricos e protocolos de transmissão. Estes cartões operam com proximidade máxima de dez centímetros.

2.3.2.5. ISO/IEC 10536

Cartões do tipo "close-coupled" - especificamente estabelecem padrões para características físicas, dimensões e localização das áreas de acoplamento, sinais elétricos e procedimentos de reset.

2.3.2.6. ISO/IEC 15693

Cartões do tipo "vicinity" - especificamente estabelecem padrões para as características físicas, energia por radio freqüência, sinais de interface. Estes cartões operam com distância máxima de um metro.

2.3.2.7. ISO/IEC 7501

Descreve padrões para máquinas de leitura para documentos de viajem e fornece recomendações claras sobre a topologia de smart cards.

2.3.3. Normas e Padrões para Avaliação de Segurança

2.3.3.1. ISO/IEC 15408 (Common Criteria)

O Common Criteria (CC) aplica-se de modo a prover uma padronização para prover uma avaliação de segurança para produtos e sistemas de Tecnologia da Informação. O CC visa desenvolver níveis de segurança que determinam os requisitos e alvos de segurança para um determinado sistema de informação. O CC foi desenvolvido por uma organização patrocinada pelos Estados Unidos, Canadá e Europa. Essa organização iniciou o desenvolvimento do Common Criteria em 1993. Em 1996, o Commom Criteria v1.0 foi produzido. Em 1998 foi editada a v2.0 e em 1999 a versão mais recente, v2.1, serviu de base para a ISO/IEC 15408.

O Common Criteria (CC) é um padrão internacional voltado para a área de segurança na computação. Diferente de outros padrões como FIPS 140, o Common Criteria não provê uma lista de requisitos de segurança do produto, ou recursos que os produtos devem conter. Ao invés disso, provê uma camada base na qual os fabricantes podem especificar os seus próprios requisitos de segurança ou implementar ou aclamar sobre os atributos de segurança

de seus próprios produtos. Os laboratórios de testes podem avaliar os produtos para determinar se realmente os produtos atendem a esses atributos.

Em outras palavras, o Common Criteria provê a garantia de que o processo de especificação, implementação e avaliação dos atributos de segurança do produto foi conduzida de uma maneira rigorosa.

O Common Criteria possui diversos elementos:

- Target Of Evaluation (TOE) – o produto ou sistema sujeito à avaliação.
- Protection Profile (PP) – um documento, geralmente elaborado pelo usuário ou por uma comunidade, que identificam os requisitos de segurança relevantes para um propósito particular.
- Security Functional Requiriments (SFRs) – especifica individualmente as funções de segurança aos quais podem ser providos pelo produto.
- Security Target (ST) – o documento que especifica as propriedades de segurança do TOE.
- O Evaluation Assurance Level (EAL) é uma atribuição numérica dada ao produto avaliado que reflete a conformidade dos requisitos qualificados durante a avaliação. Cada EAL corresponde a um pacote de requisitos garantidos que cobrem o desenvolvimento completo do produto, com um determinado nível de conformidade. O Common Criteria é composto por sete níveis, sendo o EAL1 o nível mais baixo e o EAL7 o nível mais elevado. Um nível maior não implica necessariamente em uma melhor segurança, apenas indica que o produto foi avaliado por um processo mais rigoroso.

Existem diversas características que indicam superioridade em relação a outros processos de avaliação de segurança. Primeiro, o Common Criteria foi desenvolvido combinando as melhores práticas dos padrões de segurança existentes em seis países. Quatorze países assinaram um tratado reconhecendo o Common Criteria como um padrão de avaliação de segurança de alta qualidade.

Segundo, o Common Criteria estabelece e mantém padrões rigorosos para os critérios de avaliação, bem como para a condução dos testes. Qualquer laboratório que deseja conduzir uma avaliação do Common Criteria precisa ser certificads através de um rigoroso processo, com inspeção periódica.

Terceiro e o mais importante, todas as avaliações feitas pelos laboratórios são enviadas ao laboratório Common Criteria do país para verificar se todo o processo foi seguido corretamente, para reforçar a consistência entre os laboratórios e prevenir qualquer incentivo financeiro externo para influenciar os resultados da avaliação.

2.3.3.2. Federal Information Processing Standard (FIPS) 140

O Federal Information Processing Standard (FIPS) 140 é um padrão elaborado pelos Estados Unidos em conjunto com o governo do Canadá que especifica requisitos de segurança em módulos criptográficos. O FIPS 140 possui quatro níveis de garantia: o nível 1 é o menos rigoroso e o nível 4 é o mais elevado. Cada nível é a extensão do nível abaixo, logo, ter um certificado de nível 2 significa atender aos requisitos para ambos os níveis: 1 e 2.

- Nível 1: o mais baixo, impõe requisitos muito limitados; de uma forma geral, todos os componentes devem ser reconhecidos como “produtos” e diversos problemas graves de segurança devem estar ausentes.

- Nível 2: adiciona requisitos para evitar a violação do hardware (tamper evidence) e autenticação falsa.

- Nível 3: adiciona requisitos para resistir à violação do hardware (tornando o acesso à informação contida no chip mais difícil), garantir a autenticação e garantir uma separação física e lógica entre as interfaces cujos parâmetros críticos de segurança entrem ou saiam do módulo.

- Nível 4: faz com que os requisitos de segurança física sejam mais rigorosos, impondo maior resistência contra ataques externos.

Os testes para certificação FIPS 140 são feitos por laboratórios independentes que foram previamente certificados para tal propósito. Os resultados são encaminhados para o

NIST[2] (National Institute of Standards and Technology) nos Estados Unidos e para o Canadian Security Establishment (CSE) no Canadá para uma validação independente.

Assim como na certificação Common Criteria, o processo seguido para o FIPS 140 vem de padrões rigorosos tanto para os testes do módulo quanto para o laboratório que conduz os testes, combinados com a validação independente dos resultados dos testes.

A revisão 2 do FIPS 140 (FIPS 140-2) incorpora mudanças na aplicação dos padrões e tecnologia desde o desenvolvimento da sua primeira revisão (FIPS 140-1), assim como mudanças baseadas nos comentários de fornecedores, laboratórios e comunidades de usuários.

2.3.4. Normas e Padrões para Criptografia e Certificação Digital

2.3.4.1. Padrões FIPS para Criptografia

São desenvolvidos pela Computer Security Division dentro da NIST[2] norte americana. Os padrões FIPS são desenhados para proteger os sistemas de computação e de telecomunicações norte americanos. Os padrões FIPS são aplicados nos smart cards no que diz respeito aos padrões de assinatura digital, padrões de criptografia e requisitos de segurança para os módulos criptográficos. Neste aspecto, alguns padrões devem ser considerados para desenvolvimento dos módulos criptográficos embarcados em smart cards, e seu uso em aplicações:

- Assinaturas digitais e padrões de criptografia
    - FIPS 186-2 – especifica o conjunto de algoritmos utilizados para geração e verificação de assinaturas digitais. Esta especificação relaciona três algoritmos especificamente: Digital Signature Algorithm (DAS), RSA, e o algoritmo para assinatura digital de curvas elípticas (ECDSA);
    - ANSI X9.31-1998 - contém especificações para o algoritmo RSA. O padrão cobre especificamente o gerenciamento manual e automático de

[2] NIST é uma agência do United States Departament's Technology Administration

chaves usando na criptografia assimétrica e simétrica para a indústria nos serviços financeiros de venda no atacado;

- ANSI X9.62-1998 - contém especificações para o algoritmo de assinatura ECDSA.

- FIPS 197: O Advanced Encryption Standard (AES) é um algoritmo de criptografia simétrica aprovado pela FIPS.

- Requisitos de segurança para módulos criptográficos

  - O FIPS 140 (1-3) descreve as áreas relacionadas à segurança no desenvolvimento e implementação dos módulos criptográficos, especialmente: especificação do módulo criptográfico, portas e interfaces; regras, serviços e autenticação; modelo de estado finito; segurança física; ambiente operacional; gerenciamento de chaves criptográficas; interferências eletromagnéticas compatíveis com (EMI/EMC); auto testes; garantia de projeto; e considerações para minimização de ataques.

2.3.4.2. Public Key Cryptography Standards (PKCS)

PKCS (Public Key Cryptography Standards) é o conjunto de especificações criadas para padronizar os formatos e operações de criptografia. Foram produzidas pelos Laboratórios RSA em cooperação com desenvolvedores de sistemas de segurança com o propósito de acelerar a implementação da criptografia assimétrica.

- PKCS#1: RSA Encryption Standard. Especifica o padrão de dados para o protocolo RSA, incluindo o padrão para criptografia e assinatura digital RSA e padrão para estocagem de chaves públicas e privadas.

- PKCS#3: Diffie-Hellman Key Agreement Standard. Descreve o método para implementação de chaves no Diffie-Hellman, cujo objetivo é fornecer protocolos para estabelecimento de conexões seguras.

- PKCS#5: Password-Based Encryption Standard. Especifica um padrão para proteção de dados para se usar a criptografia em senha com o DES.

- PKCS#6: Extended-Certificate Syntax Standard. PKCS#7: Cryptographic Message Syntax Standard. Descreve uma sintaxe geral para os dados serem criptografados e aplicados em assinaturas digitais e mensagens digitais. Toma como base a RFC 2630. É utilizado para prover mensagens seguras em S/MIME.

- PKCS#8: Private-Key Information Syntax Standard. Especifica um padrão para estocagem de chaves privadas, incluindo a vantagem de criptografá-las com PKCS#5.

- PKCS#10: Certification Request Syntax Standard. Especifica um padrão para codificar requisições de certificados, incluindo o nome da pessoa que requisita o certificado e sua chave pública.

- PKCS#11: Cryptographic Token Interface Standard. Descreve a interface de programação chamada "Cryptoki" utilizada para operações criptográficas em hardwares: tokens, cartões inteligentes.

- PKCS#12: Personal Information Exchange Syntax Standard. Define o formato para armazenamento e transporte de chaves privadas, certificados, entre outros.

- PKCS#13: Elliptic Curve Cryptography Standard. Padroniza algoritmos de criptografia baseado em curvas elípticas, incluindo o formato, a geração de validação de chaves, assinaturas digitais, etc.

- PKCS#15: Cryptographic Token Information Format Standard. É o padrão que define o uso da tecnologia de criptografia baseada em tokens.

2.3.4.3. ISO/IEC X.509

O padrão mais comumente adotado para ceritificados digitais é o padrão X.509. Com o passar do tempo foram necessárias várias adaptações neste padrão para resolver problemas de vulnerabilidade e aumentar a sua aplicabilidade:

- X.509v1: tinha um número restrito limitado de campos nesta forma de utilização. Além disso, foram identificadas vulnerabilidades.

- X.509v2: foram adicionados novos campos com o objetivo de possibilitar a reutilização de nomes iguais em diferentes certificados digitais.

- X.509v3: foram adicionados campos de extensão, tornando o certificado mais flexível.

O esquema abaixo mostra a evolução das versões do padrão X.509.

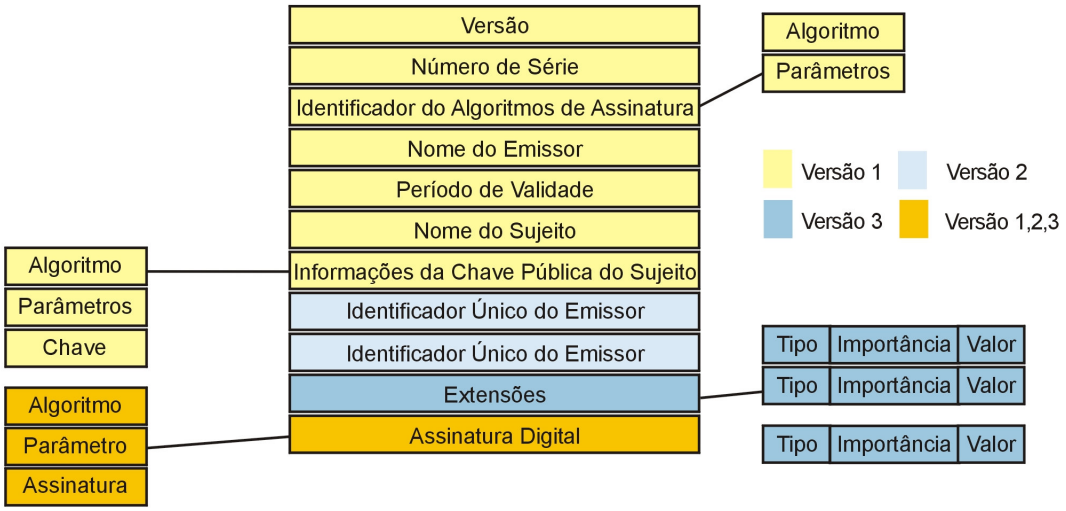


Figura 2-9 – Evolução do formato padrão X.509

Fonte: Manual de Condutas Técnicas [45]

2.3.5. Outros padrões desenvolvidos e aplicados

- **American National Standards Institute (ANSI) Standards –** são recomendações direcionadas para as necessidades do governo dos Estados Unidos supervisionando as atividades de padronização desenvolvidas por outras instituições. A ANSI não escreve ou desenvolve padrões próprios, e sim, qualquer grupo nos Estados Unidos que participe da ISO, por exemplo, deve primeiro pertencer a algum dos grupos da ANSI. O *International Committee for Information Technology Standards* (INCITS) atua como ANSI's *Technical Advisory Group* (TAG). Alguns grupos de trabalho dentro do INCITS – como o B10 (*Identification Cards and related devices)*, T6 (*Radio Frequency Identification Technology*) e M1 (*biometrics*) contribuem diretamento para para os grupos de trabalho da ISO (especialmente o ISO/IEC *Joint Technical Committee 1/Subcommittee* 17 (JTC 1/SC 17)).

- **Global Platform (GP) -** é uma associação não comercial. Seu objetivo é criar e promover especificações da tecnologia de *smart card*, incluindo especificações para os cartões, componentes de hardware para *smart card* e sistemas. No mundo

existem aproximadamente vinte milhões de indivíduos usando *smart card* que foram implementados usando as especificações da GP e estão presentes nas indústrias de varejo, saúde, governo, financeiro e telefonia móvel. A estratégia do GP e de criar sistemas que são interoperáveis, compatíveis e baseados em padrões.

- **Especificações *Security Equipment Integration Working Group* (SEIWG) 012** – esta especificação estabelece requisitos para desempenho, estrutura, manufatura, testes e aceitação para cartões de tarja magnética – *Magnetic Stripe Credential* (MSC) para certas implementações de aplicações para governo. O SEIWG-012 determina que uma credencial de quarenta dígitos ou "identificador único" deve ser embarcada em todos os cartões de controle de acesso que tenha uma tarja magnética. Este "identificador único" e formado por esquema de numeração de quarenta dígitos. Esta especificação inicialmente, fora inicialmente aplicada apenas a cartões de tarja magnética porque, até então, estes eram os únicos cartões que possuíam capacidade de armazenamento suficiente para comportar esta especificação. Atualmente, a tecnologia dos *smart cards* prevaleceu, a especificação SEIWG-012 foi aplicada muito bem nesta tecnologia, pois estes dispositivos são capazes de armazenar de maneira segura essas credenciais de quarenta dígitos, e as leitoras de ler esta informação de maneira segura.

- **International Civil Aviation Organization (ICAO)** – O ICAO é responsável por fornecimento de padrões e especificações para *Machine Readable Travel Documents* (MRTD) – exemplos: passaportes, vistos e documentos de viajem. As atuais especificações não incluem o uso de *smart cards*, o ICAO ainda estuda essa possibilidade, aonde existe uma tendência para o uso de *smart card* do tipo "*contactless"*.

- **International Airline and Transportation Association (IATA) –** desenvolve padrões e recomendações para a indústria de transporte aéreo. A IATA conduz uma força tarefa para desenvolver padrões de interoperabilidade para *tiketless* baseados em *smart card*. Sua missão e assegurar uma fácil e conveniente negociação com as empresas de *tikets* eletrônicos aéreos.

- **G-8 Health Standards –** vem em conjunto para desenvolver um padrão para formato de dados de cartões de saúde. Este padrão tenta criar interoperabilidade

para os cartões de saúde dos paises do G-8. Tem seu foco em dados como: formato de arquivos para endereços, como os dados são armazenados no cartão e o uso de certificados digitais na área de saúde.

- **The Health Insurance Portability and Accountability Act (HIPAA) of 1996 –** é uma lei desenvolvida pelos Estados Unidos e mantida pelo *Department of Health and Human Services* (HHS), seu objetivo e adotar padrões nacionais para a implementação de sistemas de informação para transações eletrônicas de informação em saúde. Exemplos dessas transações incluem:

- **Global System for Mobile Communication (GSM) Standards** – são os padrões para sistemas de telefonia celular, tendo com objetivo primário oferecer compatibilidade internacional. As especificações atrelam o número do telefone a um *smart card*, chamado de SIM – *Subscriber Identification Module* ou UIM – *User Identity Module*, que são instalados nos aparelhos celulares, aonde é necessário a inserção do SIM para ativação do telefone.

- **EMV 2000 Specifications** – Para garantir interoperabilidade global em transações eletrônica financeira de crédito e débito com o uso dos *smart card*, a Europay, Mastercard e Visa (EMV), publicou a primeira versão do seu padrão para cartão e terminal de transação em 1995. As especificações são construídas com base da ISO/IEC 7816 e funciona como uma expansão para acomodar transações eletrônicas financeiras. Em dezembro de 2000 foi publicada a versão EMV 2000 versão 4.0 que consiste em quatro livros:

    - Livro 1 – descreve funcionalidades mínimas requeridas para *smart cards* e terminal de transações para garantir operações corretas e interoperabilidade independente da aplicação que se esteja utilizando;

    - Livro 2 – *Security and Key Managements* – descreve os funcionalidade mínimas de segurança para *smart cards* e terminais de transação para garantir operações corretas e interoperabilidade. Funcionalidades adicionais e recomendação são providas sobre a comunicação online entre o *smat card*, emissão e o gerenciamento de chaves criptográficas no terminal de transações, emissor e sistema de pagamento;

- Livro 3 – *Application Specification* – define os procedimentos necessários nos terminais de transação e *smart card* para realização de uma transação em sistemas de pagamento em um cenário internacional;

- Livro 4 - *Cardholder, Attendant, and Acquirer Interface Requirementsi* – define requisitos mandatórios, recomendações, e requisitos opcionais necessários para aceitação de *smart cards* e terminais de transação em concordância com os livros 1, 2 e 3.

- **A Smart Card Alliance** – é uma organização sem fins lucrativos, formado pela associação de *players* da indústria para acelerar e expandir a aceitação de múltiplas aplicações com o uso de *smart cards*. É composto por lideres da indústria de tecnologia incluindo os segmentos bancários, financeiros, computação, telecomunicação, tecnologia, saúde, varejo e indústria de entretenimento bem como agencias governamentais. Tem o objetivo de convergir os lideres da indústria para o desenvolvimento de novas gerações de produtos e serviços baseados no uso da tecnologia de *smart cards*.

- **O PC/SC Workgroup** – Foi formado em 1996 e inclui a Schlumberger Eletronics Transactions, Bull CP8, Hewlett Packard, Microsoft e outros líderes de mercados. Este grupo vem desenvolvendo especificações abertas para a integração do *smart card* com os computadores pessoais. As especificações têm base na independência de plataforma e padrões existentes na indústria, são desenhadas para possibilitar o desenvolvimento de aplicações baseadas em *smart card* aplicadas em sistemas bancários seguros, saúde, segurança corporativa e comércio eletrônico, incluem ainda, funcionalidade criptográficas e armazenamento seguro, interfaces de programação para leitores de *smart card* e PCs, e uma interface de alto nível para o desenvolvimento de aplicações. Vale dizer que as especificações do PC/SC são baseadas no padrão ISO/IEC 7816 e suporta as especificações EMV e GSM.

- **OpenCard™ Framework** – é um conjunto de guias anunciado pela IBM, Netscape, NCI e Sun Microsystem para a integração dos *smart cards* com as redes de computadores. Estes guias são baseados em padrões abertos e provem uma arquitetura e um conjunto de interfaces de programação para aplicação (APIs) que possibilitam o desenvolvedores de aplicação e provedores de serviço construir e

implementar soluções com *smart card* em qualquer rede de computadores que estiver aderido ao OpenCard. A fim de prover uma interface de alto nível que suporte vários tipos de *smart cards*, a OpenCard Framework permite uma interoperabilidade independente do fornecedor de *smart card*. Os guias incorporam o padrão PKCS#11 e outros mecanismos de chave pública.

- **Java Card** – é um conjunto de especificações para rodar um subconjunto de Java em um *smart card*.

- **JCF (Java Card Forum)** – é uma associação da indústria focada no avanço das especificações do Java Card para servir ao mercado.

- **JCRE (Java Card Runtime Environment)** – é um ambiente *run-time* para gerenciar operações como leitura e inicialização de *applets* Java

- **Jini** – é um *framework* de computação distribuída introduzido pela Sun Microsystem.

- **MIDlet (Mobile Information Device Applet)** – Um *Applet* desenvolvido para rodar em aparelho móvel.

- **CAP file (Converted Applet File)** – é um arquivo produzido quando um arquivo de classe Java e convertido para ser lido por um Java *Card*.

- **KVM (K Virtual Machine)** - Uma máquina virtual Java desenvolvida para aparelhos móveis.

2.3.6. Posicionamento Brasileiro

O Comitê Gestor da infra-estrutura de Chaves Públicas Brasileira aprovou em 21 de outubro de 2004, por meio da Resolução n o 36 de 21/10/2004, o regulamento para homologação de sistemas e equipamentos de certificação digital no âmbito da ICPBrasil. O Instituto Nacional de Tecnologia da Informação (ITI), enquanto Autoridade Certificadora Raiz da ICPBrasil, será responsável pela condução desses processos.

Segundo a Resolução, os smart cards deverão obedecer a padrões e especificações técnicas mínimas, a fim de garantir a sua interoperabilidade e a confiabilidade dos recursos de segurança da informação por eles utilizados.

As especificações e padrões a serem seguidos encontram-se em Manuais de Condutas Técnicas, disponíveis na internet através do endereço: http://www.lea.gov.br. Nos manuais vê-se claramente a intenção brasileira de seguir rigorosamente os padrões internacionais afim de conseguir uma interoperabilidade entre fabricantes nacionais e estrangeiros. Os padrões contemplados nos manuais são, entre outros, a ISO 7816 e a PC/SC versão 1.0.

Em relação aos requisitos de segurança o Brasil obedece ao padrão FIPS 140-2[3].

O padrão de interoperabilidade para módulos criptográficos[4] no Brasil obedece à seguinte estrutura, mostrada na Figura 2-10.

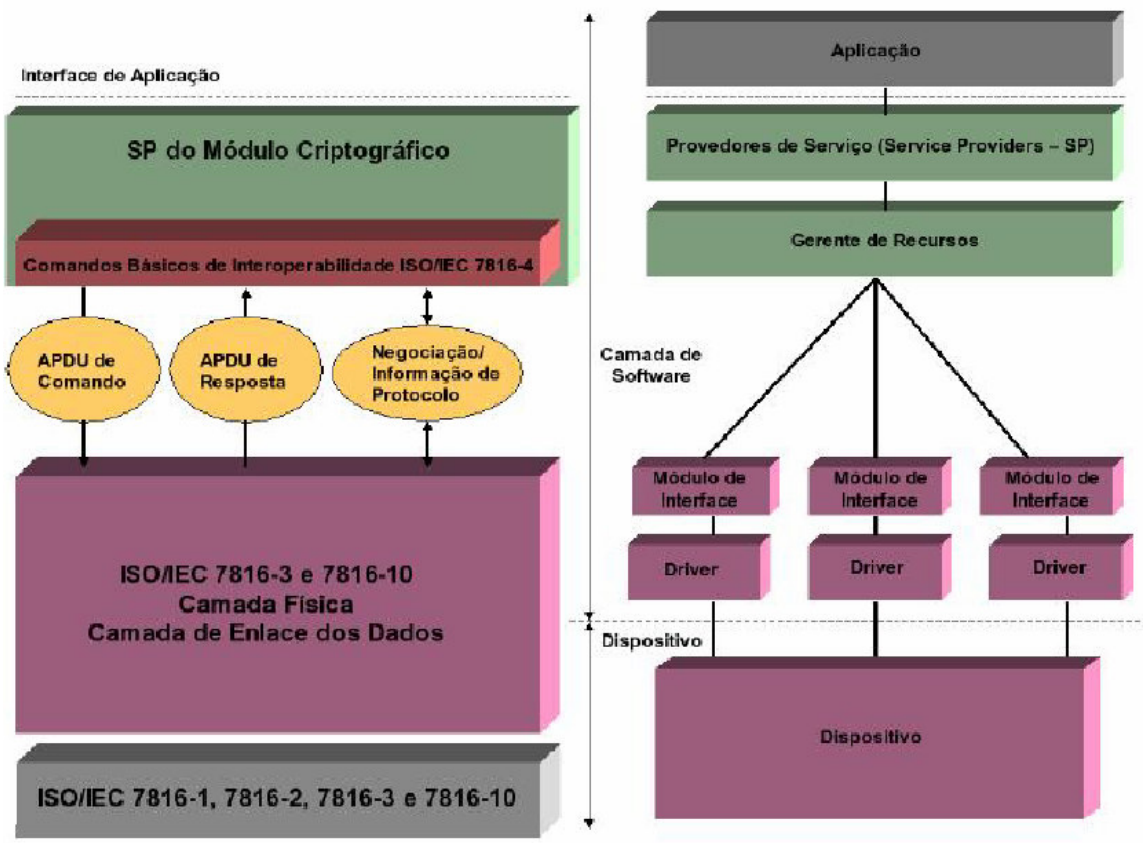


Figura 2-10 - Arquitetura Padrão de Interoperabilidade Brasileira

Fonte: Manual de Condutas Técnicas [45]

[3] O padrão FIPS 140-2 abrange diferentes áreas de atuação relacionadas ao projeto e implementação de um módulo criptográfico: Especificação do módulo criptográfico; suas portas e interfaces; papéis, serviços e autenticação; segurança física e ambiente operacional.

[4] Cryptographic Module: Conjunto de hardware, software e/ou firmware que implementa funções ou processos criptográficos, abrangendo algoritmos criptográficos e de gera¸cão de chaves. No escopo do Manual de Condutas Técnicas abrange não só smart cards, mas também tokens.

Os smart cards e leitores são passíveis de homologação, ganhando um selo de qualidade. Os produtos homologados por esse processo terão um laudo de conformidade emitido e utilizarão o selo de homologação e seu correspondente número de identificação.

2.4. SISTEMAS OPERACIONAIS DE SMART CARDS

Apesar de ser um pequeno programa no microprocessador de um smart card, esse programa pode ser chamado de um Sistema Operacional. De acordo com o padrão alemão DIN 44300, um sistema operacional é definido como "os programas de um sistema de computador digital que, juntamente com as propriedades do sistema de computação forma a base de modos de operações possíveis do sistema de computação pessoal, particularmente no controle e monitoração da execução do programa". Dessa maneira, o termo "sistema operacional" independe do tamanho, referindo-se somente às funções do programa. Os sistemas operacionais para smart cards são desenvolvidos para operar como uma interface serial bidirecional para o terminal.

Um sistema operacional provê uma interface entre o hardware do computador e o software de aplicação utilizado no momento, de maneira que torna desnecessário que o software de aplicação acesse diretamente o hardware. Este é um benefício significante, já que provê à aplicação certa portabilidade.

Nos anos 90, de acordo com Rankl & Effing [58], haviam poucos sistemas operacionais de smart cards. A capacidade de memória dos cartões era pequena. A situação usual não era a presença de um sistema operacional como uma coleção bem estruturada de rotinas na memória ROM, que era utilizada quando necessário por uma aplicação particular quando o cartão estava completo. A estrutura desses sistemas era muito monolítica, e somente poderia ser modificada a altos custos. As próximas gerações começaram a ser construídas como um sistema operacional em camadas, e, nos dias de hoje, os sistemas operacionais possuem essa estrutura em camadas, além de inumeráveis refinamentos. A base para a padronização dos sistemas operacionais para smart cards é formada pela família ISO/IEC 7816, além de especificações UICC (TS 102.221) e EMV[5].

[5] Padrão desenvolvido por um consórcio entre Europay, MasterCard e Visa.

Os sistemas operacionais de smart cards, em contraste com os sistemas operacionais comuns, não incluem interfaces com usuários nem a possibilidade de acesso a mídias de memória externas. Isso ocorre porque eles são otimizados para funcionalidades completamente diferentes [54]. A segurança durante a execução do programa e o acesso protegido aos dados devem ter a maior prioridade. Como a me-mória disponível é limitada, esses sistemas operacionais possuem pequenos códigos de programas, que normalmente está na faixa de 3-250kB.

Os módulos de programas são escritos em códigos ROM. Esse fato limita as técnicas de programação que podem ser utilizadas. O fato de que o código está armazenado em ROM também explica porque alterações não podem ser realizadas uma vez que o microcontrolador foi programado e produzido. Corrigir um erro, por exemplo, pode levar de 10 a 12 semanas [66]. O tempo de testes e controle de qualidade geralmente é bem superior ao tempo de desenvolvimento do programa.

Esses sistemas operacionais devem, além de possuir poucos erros, ser confiáveis e robustos. Quebras do sistema ou respostas imprevisíveis a um comando incorreto ou a falha de uma página EEPROM não devem ocorrer sob nenhuma circunstância. Por razões de segurança, um sistema operacional de smart card deve ser produzido de acordo com o hardware do microcontrolador utilizado. Consequentemente, ele nunca pode ser totalmente independente do hardware.

Os sistemas operacionais de smart cards não possuem capacidade de multi-tarefa. As principais tarefas de um sistema operacional de smart card são as seguintes:

- Transferência de dados do smart card e para ele.
- Controle da execução de comandos.
- Gerenciamento de arquivos.
- Gerenciamento e execução de algoritmos criptográficos.
- Gerenciamento e execução de códigos de programa.

2.4.1. Processamento de Comandos

A Figura 2-11, mostra a organização do proces-samento de comandos em smart cards que não suportam códigos de programa passíveis de serem baixados. O smart card recebe cada comando pela interface serial I/O. O gerenciador de I/O realiza a detecção e correção de erros, quando necessário, de maneira independente da realizada em camadas de níveis superiores. Depois que um comando é recebido completamente, e sem erros, o gerenciador de mensagens seguras deve decifrar a mensagem criptografada ou testar sua integridade. Se a transmissão de dados segura não é utilizada, esse gerenciador é completamente transparente, tanto para o comando quanto para a resposta.

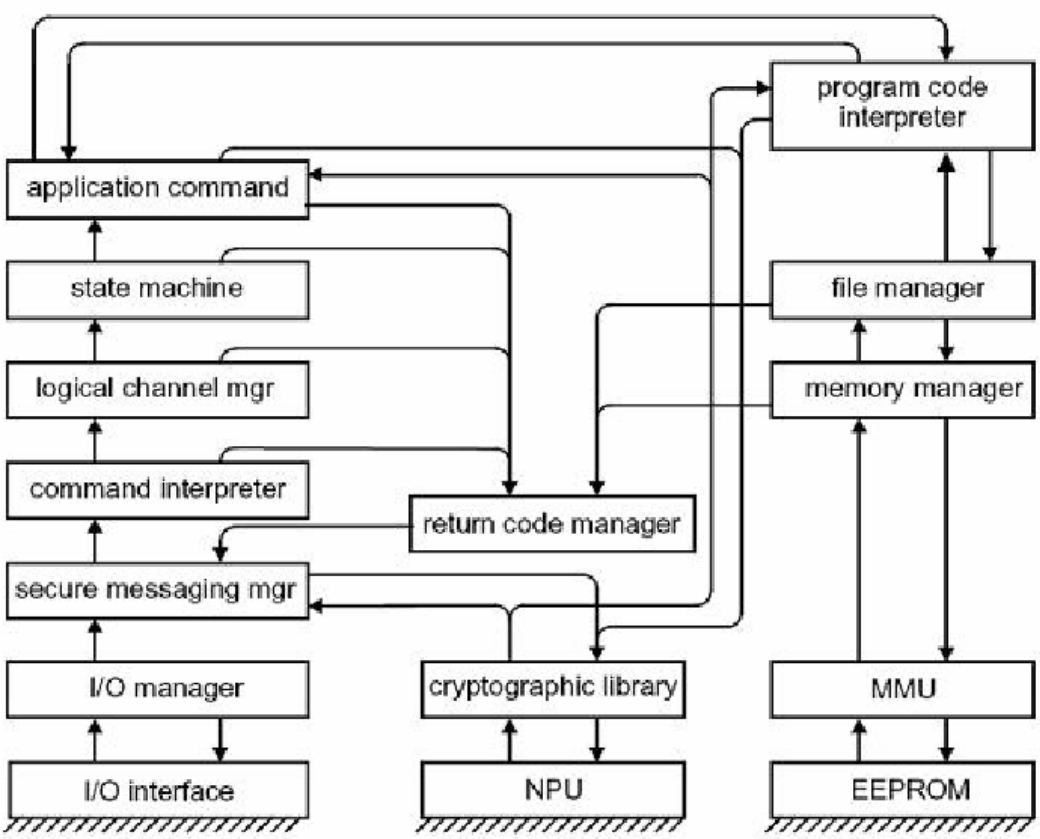


Figura 2-11 - Processamento de comandos em sistema operacional de smart card

Fonte: adaptado de Rankl & Effing [58]

Após esse processo, o interpretador de comandos tentará decodificar o comando. Se isso não for possível, é chamado o gerenciador de código de retorno. Se o comando pôde ser decodificado, o gerenciador de canal lógico determina qual canal deverá ser selecionado, muda para o estado desse canal e, se nenhum erro ocorrer, chama a máquina de estados.

A máquina de estados checa se o comando, em combinação com seus parâmetros de acompanhamento, é permitido no estado presente do smart card. Se sim, o código de programa da aplicação que processa o comando recebido é executado. Se o comando é proibido no estado corrente, ou se os valores desse parâmetro não estão reservados, o terminal recebe uma mensagem com essa resposta através do gerenciador de retorno de código e do gerenciador de I/O.

Se for necessário acessar um arquivo durante o processamento do comando, isso ocorre somente através do gerenciador de arquivos, que converte todos os endereços lógicos em endereços físicos dentro do chip. O gerenciador de arquivos também monitora todos os endereços referentes a regiões limites, e testa as condições de acesso ao arquivo em questão.

O gerenciador de arquivos utiliza um gerenciador de memória de mais baixo nível, que executa todas as funções para os endereços físicos da EEPROM. Isso garante que esse módulo do programa é o único que utiliza endereços físicos, o que incrementa significativamente a portabilidade e a segurança de todo o sistema operacional.

Um gerenciador de código de retorno central é responsável por gerar o código de retorno. Ele sempre produz a resposta completa enviada para a rotina chamada. Este nível é responsável pelo gerenciamento e geração do código de retorno utilizado em todas as outras partes do sistema operacional.

Uma vez que os sistemas operacionais de smart cards utilizam funções de criptografia, geralmente existe uma biblioteca dedicada de funções criptográficas, separada do restante do sistema operacional. Essa biblioteca serve a todos os outros módulos, como um departamento central de funções criptográficas.

Além desses níveis, uma rotina de interpretação ou verificação para arquivos executáveis deve estar presente na região acima do nível de comando da aplicação. Ele monitora os programas contidos nesses arquivos, roda-os e os interpreta. O projeto exato e a implementação dependem de onde existe algum código executável presente, e de se o código armazenado é um código de máquina ou um código a ser interpretado.

2.4.2. Perfis de Smart Cards

Nem sempre todos os comandos padronizados e as estruturas de arquivos são implementados em um sistema operacional de smart card, já que a memória disponível nesse caso é muito menor que de um PC, por exemplo. Nesse caso, "perfis" para smart cards são incluídos em dois padrões relevantes (EM 726-3 e ISO/IEC 7816-4). Cada perfil define um subconjunto de comandos e estruturas de arquivos para o padrão em questão.

Um smart card que utiliza um certo perfil deve ao menos incorporar o subconjunto definido para aquele perfil. Entretanto, esses padrões representam apenas recomendações para os desenvolvedores de sistemas operacionais. Os cinco perfis definidos na ISO/IEC 7816-4 estão mostrados na Tabela 2.3:

Os sistemas operacionais comerciais normalmente suportam vários tipos de microcontroladores, com diversas quantidades de memória disponíveis. Consequentemente, existem, na prática, perfis de sistemas operacionais que especificam certas funções, dependendo do tipo de chip. Esses perfis no sistema operacional são normalmente projetados para que as aplicações possam ser migradas facilmente, pelo menos de uma memória menor para uma maior, sem mudanças nos comandos ou na estrutura dos arquivos.

2.4.3. Arquivos em Smart Cards

A função primária dos smart cards era a de armazenamento de dados. Nesse sentido, eles possuem vantagens sobre outras mídias de armazenamento de dados, como os disquetes, em que o acesso aos dados pode ser dependente de certas condições necessárias.

Os primeiros smart cards possuíam apenas regiões de endereçamento direto à memória, que poderia ser usada para leitura ou escrita de dados. Os dados eram acessados por endereços de memória especificamente físicos. Atualmente, os smart cards possuem um sistema de gerenciamento de arquivos hierárquico completo com endereçamento simbólico e independente do hardware. Esse gerenciamento de arquivos possui características específicas aos smart cards. A característica mais óbvia é que não existe interface homem-máquina [3]. Todos os arquivos são endereçados usando código hexadecimal, e todos os comandos são baseados estritamente nesse endereçamento, já que a comunicação existe apenas entre dois computadores. É típico desse tipo de gerenciamento de arquivos o fato de que ele deve ser projetado para usar pequenas quantidades de memória.

Tabela 2-4 - Descrição dos perfis de smart cards definidos na ISO/IEC 7816-4

PERFIL	DESCRIÇÃO	
M	Estrutura do Arquivo:	• Transparente; • Linear Fixo;
	Comandos:	• READ BINARY, UPDATE BINARY Sem seleção implícita; comprimento máx. 256 bytes; • READ RECORD, UPDATE RECORD Sem seleção implícita; • SELECT FILE Com explícita especificação da FID; • VERIFY • INTERNAL AUTHENTICATE;
N	Igual ao perfil M, com o uso suplementar de um nome DF para SELECT FILE	
O	Estrutura do Arquivo:	• Transparente; • Linear Fixo; • Linear Variável; • Cíclico;
	Comandos:	• READ BINARY, UPDATE BINARY Sem seleção implícita; comprimento máx. 256 bytes; • READ RECORD, UPDATE RECORD Sem seleção implícita; • SELECT FILE • VERIFY • INTERNAL AUTHENTICATE; • EXTERNAL AUTHENTICATE; • APPEND RECORD; • GET CHALLENGE;
P	Estrutura do Arquivo:	• Transparente;
	Comandos:	• READ BINARY, UPDATE BINARY Sem seleção implícita; comprimento máx. 64 bytes; • SELECT FILE Com especificação explícita do nome DF; • VERIFY • INTERNAL AUTHENTICATE;
Q	Transmissão de Dados:	• Mensagem Segura;
	Estrutura do Arquivo:	-
	Comandos:	• GET DATA • PUT DATA • SELECT FILE Com especificação explícita do nome DF; • VERIFY • INTERNAL AUTHENTICATE; • EXTERNAL AUTHENTICATE; • GET CHALLENGE;

Fonte: adaptado de Rankl & Effing [58]

2.4.3.1. Estrutura Interna dos Arquivos

Os sistemas modernos de gerenciamento de arquivos para smart cards possuem uma estrutura orientada a objeto. Isso significa que todas as informações sobre um arquivo estão contidas no próprio arquivo. Uma conseqüência desse fato é que o arquivo necessita sempre ser selecionado, antes que qualquer ação possa ser executada. Arquivos em sistemas orientados a objetos são divididos em duas partes. A primeira parte, chamada de cabeçalho, contém informações sobre o layout e a estrutura do arquivo, e as condições de acesso a este. A segunda parte contém os dados modificáveis e é chamada de corpo do arquivo. As duas partes são ligadas entre si através de um ponteiro.

2.4.3.2. Tipos de Arquivos

A estrutura de um sistema de arquivos de smart card (Figura 2-12), como especificada na ISO/IEC 7816-4, é similar àquela de um sistema DOS ou Unix. A maior diferença é que os smart cards não contêm arquivos específicos de aplicações. Somente as estruturas de arquivos padrão devem ser usadas em smart cards.

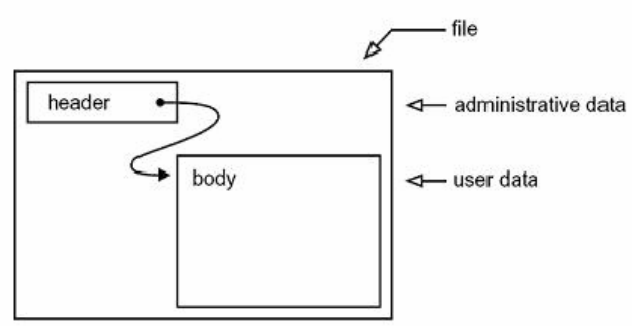


Figura 2-12 - Estrutura interna de um arquivo em um sistema de gerenciamento de arquivos de um smart card

Fonte: adaptado de Rankl & Effing [58]

Existem basicamente duas categorias de arquivos para smart cards. A primeira categoria é de arquivos de diretório, que são chamados de arquivos dedicados (do inglês, dedicated files - DF). A segunda categoria consiste nos arquivos que carregam os dados de usuário, que são chamados de arquivos elementares (do inglês, elementary files - EFs). EFs podem ser divididos naqueles utilizados pelo sistema operacional (EFs internos) e nos utilizados por aplicações externas (EFs funcionais). A Figura 2-13 ilustra essas divisões.

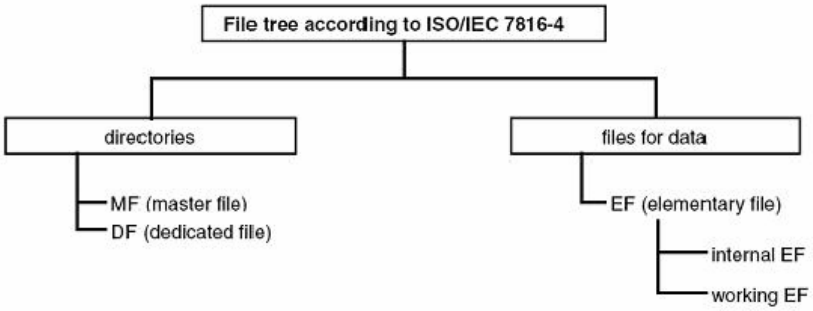


Figura 2-13 - Classificação das estruturas de arquivos de smart cards (ISO/IEC 7816-4)

Fonte: adaptado de Rankl & Effing [58]

O diretório raiz é chamado de master file (MF). Ele é automaticamente selecionado após o reset do smart card. O MF contém todos os outros diretórios e todos os arquivos. É um tipo especial de DF, e representa toda a extensão de memória disponível para a região de arquivos no smart card. Todo smart card deve conter um arquivo master.

2.4.3.3. Nomes de Arquivos

Nos sistemas operacionais de smart cards modernos, os arquivos são endereçados através de nomes lógicos, ao invés de serem acessados diretamente por endereços físicos. Apesar de demandar maior quantidade de memória, o endereçamento por nomes lógicos de arquivos é significativamente melhor, e muito mais fácil de estender. Apenas cartões de memória utilizam o endereçamento físico.

Identificador de Arquivo (FID)

Todos os arquivos, incluindo arquivos de diretório, possuem um identificador de arquivo (FID), de 2 bytes, que pode ser utilizado para selecionar um arquivo. O FID do MF é '3F00'. O endereço lógico 'FFFF' é reservado para aplicações futuras, e não deve ser utilizado. Outros FIDs são reservados pelo padrão ISO 7816-4 e por outros padrões, conforme mostra a Tabela 2-5.

Tabela 2-5 - FIDs reservados para os principais padrões

FID	Nome e propósito	Padrão
‘2F00’	FID reservada para o arquivo EF_{DIR}, usado para guardar identificadores de aplicação (AIDs) e o caminho da aplicação associada.	ISO/IEC 7816-4
‘2F01’	FID reservada para o EF_{ATR}, que contém extensões para o ATR.	ISO/IEC 7816-4
‘3F00’	MF é a raiz do diretório para todos os arquivos de um Smartcard.	ISO/IEC 7816-4 GSM 11.11 TS 102.221 EMV
‘3FFF’	FID reservada para a seleção de de arquivo usando o caminho.	ISO/IEC 7816-4
‘FFFF’	FID reservada para uso futuro.	ISO/IEC 7816-4

Fonte: adaptado de Rankl & Effing [58]

De acordo com a ISO/IEC 7816-4, existem algumas regras em relação à escolha de um FID original, que são as seguintes:

1. todos os DFs e EFs em um mesmo diretório devem possuir diferentes FIDs.
2. diretórios aninhados (DFs) não podem possuir os mesmos FIDs.
3. um EF em um diretório (MF ou EF) não pode possuir o mesmo FID que o diretório imediatamente superior ou inferior.

Identificador de Arquivo Pequeno (SFI)

Devem ser usados para a seleção implícita de arquivo no contexto presente de um comando. São opcionais para EFs, portanto não devem ser sempre necessariamente atribuídos.

Nome DF

Um DF é um tipo de diretório ou pasta, e pode conter EFs ou DFs. Cada DF possui um “nome DF” adicionado a um FID. Como especificado na ISO/IEC 7816-4, o nome DF possui um tamanho de 1 a 16 bytes. Nomes DF geralmente só são utilizados em conjunto com AIDs (Aplication IDentifiers), como definido no padrão ISO/IEC 7816-5. Uma AID deve ter o tamanho entre 5 e 16 bytes e é composto por dois elementos de dados definidos pela ISO. A Figura 2-14 ilustra essas definições.

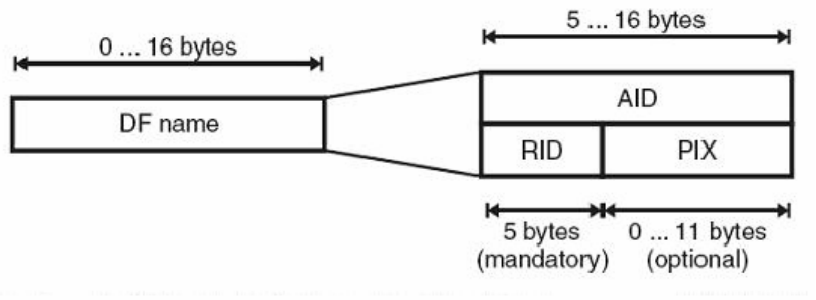


Figura 2-14 - Nome DF e AID

Fonte: adaptado de Rankl & Effing [58]

Estrutura e Codificação do Identificador da Aplicação (AID)

O identificador da aplicação (AID) consiste em dois elementos de dados. O primeiro é o RID (Registered IDentifier), que possui um tamanho fixo de 5 bytes. É atribuído por uma autoridade registradora nacional ou internacional e inclui um código do país, uma categoria da aplicação e um número que se refere ao provedor da aplicação. Cada RID é atribuído uma única vez, e esse número pode ser utilizado mundialmente para identificar uma aplicação particular. Se necessário, um provedor de aplicação pode colocar uma extensão de identificador de aplicação (PIX) após o RID.

2.4.3.4. Acesso a Recursos de Acordo com a ISO/IEC 7816-9

Os tipos de acesso a arquivos podem ser especificados usando condições de acesso orientadas a estados ou orientadas a comandos. Em condições de acesso orientadas a estado, o estado atual é comparado com a condição de acesso relevante por uma operação lógica de comparação.

Os dois tipos de condições de acesso são e continuarão a ser suportados em várias formas de sistemas operacionais de smart cards comerciais. O objetivo do padrão ISO/IEC 7816-9 é definir uma aproximação uniforme para acesso aos recursos nos smart cards e este padrão inclui uma sessão especificamente para esse fim, onde é detalhado um modelo para condições de acesso a arquivos, bem como comandos e objetos de dados (Figura 2-15).

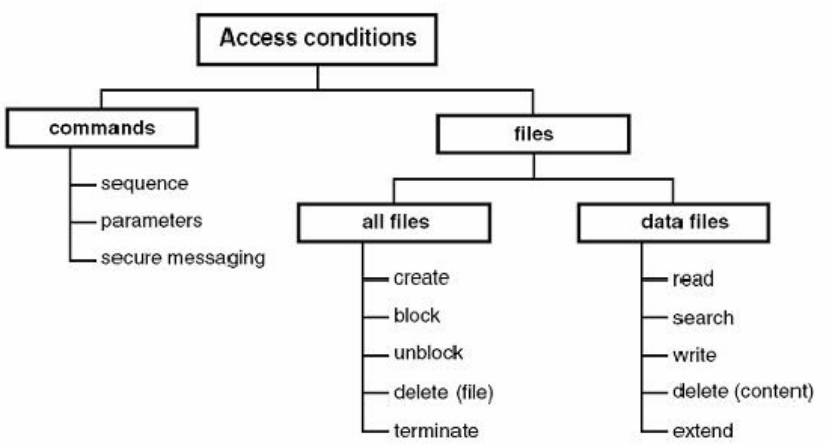


Figura 2-15 - Classificação de condições de acesso a comandos e arquivos de acordo com a ISO 7916-9

Fonte: adaptado de Rankl & Effing [58]

O padrão ISO/IEC 7816-9 define atributos de segurança, (security attributes - SA) que podem controlar acessos a recursos do cartão como arquivos, comandos ou objetos de dados, bem como a tabelas SCQL.

2.4.4. Interface PC/SC

Existe apenas um contato disponível para transmissão de dados entre o smart card e um terminal (computador pessoal, por exemplo), conforme mostrado na Figura 2-4. Cada parte transmite por vez, de maneira alternada. Esse tipo de procedimento é conhecido como half-duplex.

A comunicação com o smart card é sempre iniciada pelo PC. O cartão sempre responde a comandos do PC, o que significa que o cartão nunca transmite dados sem um estímulo. Isso caracteriza uma relação mestre-escravo, em que o terminal é o mestre e o cartão o escravo.

Após a inserção do cartão em um terminal, seus contatos são conectados mecanicamente aos contatos do terminal. Os contatos do cartão são então eletricamente alimenta-dos. O cartão então executa um reset e envia uma resposta após o reset (ATR – Response After Reset) para o terminal. O terminal avalia a ATR e então envia o primeiro comando. O cartão processa o comando e gera uma resposta, que é enviada de volta ao terminal. Esse ciclo de comandos e respostas continua até a desativação do cartão.

Entre o recebimento da ATR e o envio do primeiro comando, o terminal pode também enviar um comando de seleção de parâmetro de protocolo (PPS - Protocol Parameter Selection). O terminal pode utilizar esse comando para setar vários parâmetros de transmissão para o protocolo de transmissão do cartão. A Figura 2-16 ilustra os procedimentos descritos acima.

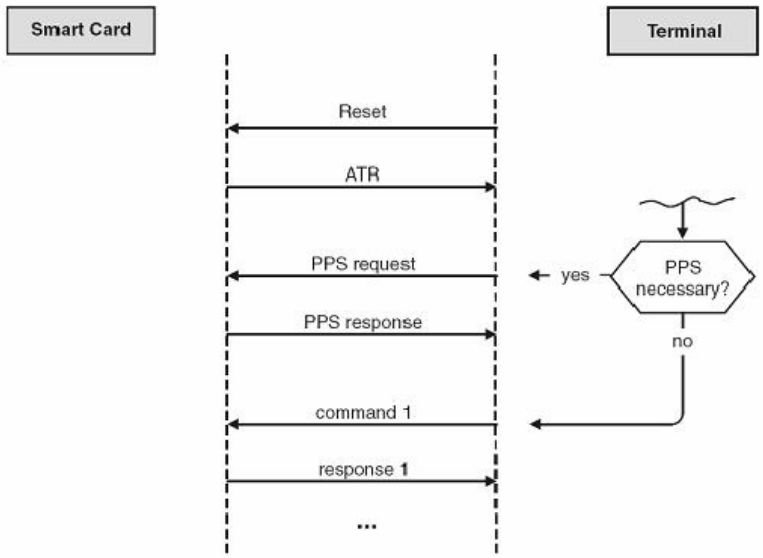


Figura 2-16 - Início da transferência de dados entre smart card e terminal

Fonte: adaptado de Rankl & Effing [58]

Os parâmetros da transmissão física entre smart cards e terminais são especificados pela ISO/IEC 7816-3. A comunicação entre os smart cards e o mundo externo deve ocorrer serialmente. Os dados tratados pelo processador em forma de bytes devem ser convertidos em seqüências de bits. Dessa maneira, cada byte é separado em 8 bits individuais, que então são transmitidos pela porta serial, um após o outro.

A transmissão de dados entre o cartão e o terminal é assíncrona, o que significa que cada byte deve conter bits de sincronização. Um start bit é adicionado ao início de cada byte transmitido, para marcar o início da transmissão para o receptor. Ao final de cada byte, a fonte adiciona também um bit de paridade para detecção de erros e um ou dois bits de parada. A paridade de cada byte deve ser sempre par. O formato do byte transmitido, bem como os bits adicionais são mostrados na Figura 2-17.

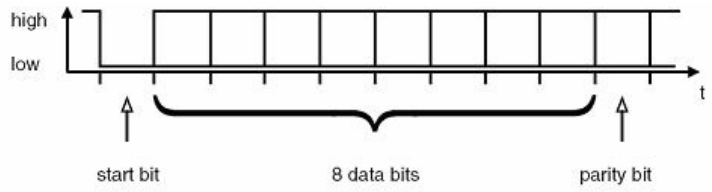


Figura 2-17 - Estrutura de um caracter para transmissão de dados

Fonte: adaptado de Rankl & Effing [58]

2.4.5. Protocolos de Transmissão

Existem várias maneiras de se estabelecer a comunicação com um smart card. Existem também diferentes métodos para ressincronizar a comunicação se uma falha ocorrer no processo. A implementação dos comandos, as respostas correspondentes a esses e os procedimentos utilizados na ocorrência de erros de transmissão são definidos por protocolos de transmissão.

Existem 15 protocolos de transmissão identificados e definidos em termos de suas funções básicas. Eles estão listados na Tabela 2-6:

Tabela 2-6 - Protocolos de transmissão de acordo com a ISO/IEC 7816-3

Protocolo	Significado
T=0	Assíncrono, half-duplex, orientado por byte, especificado na ISO/IEC 7816-3
T=1	Assíncrono, half-duplex, orientado por bloco, especificado na ISO/IEC 7816-3 Amd.1
T=2	Assíncrono, full-duplex, orientado por bloco, especificado na ISO/IEC 10536-4
T=3	Full duplex, ainda não especificado.
T=4	Assíncrono, half-duplex, orientado por byte, extensão do T=0
T=5...T=13	Reservados para uso futuro, ainda não especificados
T=14	Para uso nacional, não-escopo da ISO
T=15	Reservados para uso futuro, ainda não especificados

Fonte: adaptado de Rankl & Effing [58]

Dois desses protocolos são predominantes. São os protocolos T=0 e T=1. A principal diferença entre eles, conforme visto na tabela acima, é o fato de que o primeiro é orientado a byte e o segundo é orientado a bloco.

2.4.5.1. PROTOCOLO T=0

Utilizado inicialmente na França, foi o primeiro protocolo a ser internacionalmente padronizado. Foi desenvolvido nos primeiros anos da tecnologia de smart cards, por isso foi

projetado para uso mínimo de memória e máxima simplicidade. É utilizado mundialmente nos cartões GSM, o que o torna o protocolo mais utilizado. É padronizado pela ISO/IEC 7816-3.

É orientado a byte, o que significa que a menor unidade processada pelo protocolo é um byte simples. A unidade de dados transmitida consiste num cabeçalho contendo um byte de classe, um byte de comando e três bytes de parâmetro, opcionalmente seguidos por uma seção de dados (Figura 2-18). A detecção de erros no protocolo T=0 é baseada exclusivamente em um bit de paridade adicionado a cada byte enviado.

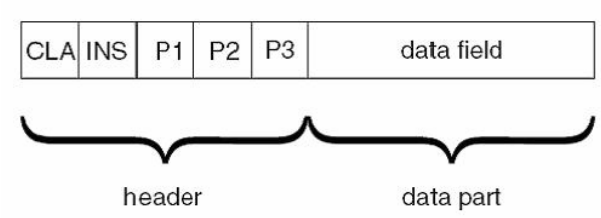


Figura 2-18 - Estrutura de um comando com protocolo T=0

Fonte: adaptado de Rankl & Effing [58]

2.4.5.2. PROTOCOLO T=1

É um protocolo half-duplex assíncrono para Smart Cards. É baseado no padrão ISO/IEC 7816-3. O protocolo T=1 é orientado a bloco, o que significa que a menor unidade de dados que pode ser transmitida entre o cartão e o terminal é um bloco.

O bloco consiste em um campo de prólogo (inicial), um campo de informação e um campo de epílogo (final). Os campos de prólogo e epílogo são mandatórios e devem ser enviados. O campo de informações é opcional e contém dados para a camada de aplicação, que é também um comando APDU enviado para o cartão ou uma resposta APDU do cartão.

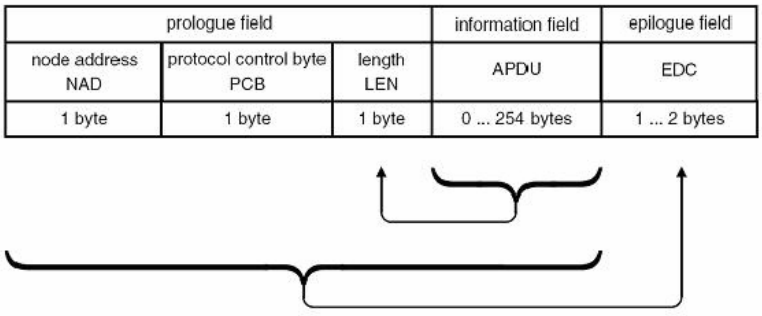


Figura 2-19 - Estrutura de um bloco de transmissão T=1

Fonte: adaptado de Rankl & Effing [58]

2.4.6. Plataformas Abertas

De acordo com Rankl & Effing [58], este termo se refere a sistemas operacionais de smart cards em que se reserva uma área para carregamento de aplicações e programas dentro dos smart cards sem a necessidade do envolvimento direto do produtor do smart card. Genericamente falando, a maioria das especificações de plataformas abertas são públicas e são geradas por um consórcio de companhias (como o Java Card Fórum). Muitos sistemas operacionais de smart card abertos são disponibilizados por vários produtores, que provêm sistemas contendo similaridade e compatibilidade entre muitas funções.

O oposto de uma plataforma aberta é uma plataforma proprietária. Este termo muitas vezes é utilizado em um sentido depreciativo por se referir a uma solução de uma única companhia. Em muitos casos, as especificações de muitas plataformas não são totalmente publicadas ou são propriedade de uma única companhia.

Muitos sistemas operacionais de smart cards chamados “abertos” são propriedade e dependentes de uma companhia específica. Plataformas verdadeiramente abertas, como no caso do Linux para PCs, com acesso livre ao código fonte, sem restrições de licenciamento e independência de companhias ou organizações não existem na área de sistemas operacionais de smart cards.

2.4.7. Sistemas Operacionais Proprietários

Sistemas Operacionais proprietários, ou nativos, se referem ao sistema desenvolvido pelo fabricante do chip que gerencia todas as aplicações e operações executadas no cartão.

Cada Sistema Operacional desenvolvido para ser executado nativamente possui suas próprias características, que podem diferir de um sistema para outro, já que o fabricante almeja extrair o melhor do chip para o seu processamento e/ou gerenciamento de memória ou baratear seu custo de produção, uma vez que não é preciso embarcar nenhuma máquina virtual na ROM do chip.

Da mesma forma encontrada em sistemas operacionais baseados em plataforma aberta, a segurança no chip também pode ser encontrada com características semelhantes como firewall entre aplicações e algoritmos de criptografia simétrica e assimétrica. Todas essas características de segurança também são analisadas por padrões de certificação de segurança.

Diferente de sistemas operacionais baseados em plataforma aberta, como o Java Card, os aplicativos em sistemas proprietários geralmente são processados de maneira mais rápida, pois não precisam ser interpretados em tempo de execução pela máquina virtual e o acesso ao hardware é feito em uma camada transparente.

Além disso, para o gerenciamento de memória, não é necessário alocar espaço, mesmo que temporariamente, na EEPROM, uma vez definidas as aplicações, os sistemas operacionais proprietários já reservam uma área na memória (não nominal) para tal propósito.

2.4.8. Plataforma Java

Java Card se refere à tecnologia que permite pequenas aplicações baseadas em Java (applets) serem executadas com segurança em Smart Cards. Amplamente utilizado em SIM Cards (usados em celulares GSM). O primeiro Java Card foi introduzido em 1997 por algumas empresas.

Os principais recursos do Java Card são: portabilidade e segurança:

- Portabilidade – a máquina virtual Java Card é responsável por interpretar os bytecodes da applet Java Card. Na teoria um applet desenvolvido para um determinado chip baseado em Java Card poderá ser executado em um outro chip com mesmas características.

- Segurança – a segurança em Java Card é baseada em diversos aspectos:

    - Encapsulamento de dados: os dados são armazenados junto com a aplicação e a aplicaçõe Java Card é executada em um ambiente isolado (máquina virtual), separado da camada do sistema operacional e da camada de hardware.

    - Applet Firewall: uma barreira lógica isola as diversas applets no Java Card. Dessa forma, uma applet não possui acesso a outra.

    - Criptografia: geralmente os algoritmos DES, 3DES, AES e RSA são usados para criptografar dados diversos.

Entretanto, Java Cards possuem um processamento mais lento comparado a cartões com sistemas operacionais proprietários uma vez que todas as applets são interpretadas em tempo de execução e convertidas para código nativo.

Além disso, a máquina virtual Java Card necessita gerenciar a memória alocada temporariamente na EEPROM, o que nos indica uma redução do espaço nominal livre da EEPROM do chip em questão.

Devido às applets serem executadas em uma camada isolada das demais, uma applet não possui acesso às demais funcionalidades nativas do sistema operacional, podendo acarretar na redução de desempenho do chip.

2.4.9. Plataforma MULTOS

MULTOS consiste em duas tecnologias que juntas possibilitam uma arquitetura segura – a máquina virtual existente no cartão que executa de forma segura as aplicações e o esquema de segurança do MULTOS, que implementa tecnologia STEP, que protege o cartão, o código da aplicação e os dados da aplicação.

As aplicações MULTOS são desenvolvidas em linguagens de alto-nível como C ou Java (ou em Assembly como linguagem de baixo-nível) e compilados para instruções MEL que são executados pela máquina virtual. Quando uma aplicação é executada, a máquina virtual verifica cada e toda instrução para assegurar sua validade e formatada corretamente. Todas as áreas de memória acessadas pelas instruções são também verificadas para assegurar de que estão dentro da área de memória da aplicação. Qualquer instrução ou tentativa de acesso à memória inválida são rejeitadas pela máquina virtual e todas as aplicações param de executar.

A verificação em tempo de execução garante segurança total na execução de aplicações bem como os seus dados – não é possível para uma aplicação acessar os dados de outra aplicação no cartão. Como o compartilhamento de dados não é permitido, os provedores de aplicações ficam seguros de que seus dados estarão seguros de outras aplicações ao longo da vida útil do cartão. O conjunto de instruções MEL é limitado à manipulação de dados e operações aritméticas simples, entretanto, os sistemas operacionais MULTOS provêm uma grande gama de funções adicionais embutidas, chamados de Primitivas, que provém operações mais complexas como criptografia ou acesso a dados do sistema operacional. A

mesma verificação no acesso à memória é feita na manipulação de áreas de memória pelas Primitivas, garantindo que as aplicações não possam acessar memória fora do espaço permitido.

2.5. OUTRAS CARACTERÍSTICAS

2.5.1. Anti-tearing

No momento em que uma informação está sendo escrita na EEPROM do chip, deve ser considerada a probabilidade de acontecer algum problema externo que interrompa a transação antes da mesma ser finalizada. De fato, a escrita pode ser interrompida por diversos eventos assíncronos, como a retirada do cartão, ou uma perturbação elétrica em alguns dos sinais (clock, reset e de alimentação). Nesse caso, pode ser que a EEPROM seja parcialmente apagada ou escrita, causando perda de dados perdidos inacessibilidade dos mesmos.

Para solucionar esse problema, um mecanismo na transação, chamado anti-tearing, deve gerenciar a escrita na EEPROM de tal forma que os dados anteriores continuem disponíveis depois da escrita de um novo dado.

Ainda mais, a atomicidade de um determinado APDU poderá ser necessária. Nesse caso, diversas escritas na EEPROM podem compor uma transação. A transação é iniciada antes da primeira escrita de um APDU e finalizada após seu término.

2.5.2. Ciclos de Leitura e Escrita

Os ciclos de leitura e escrita estão inteiramente ligados ao número de transmissões de dados entre o cartão e o leitor. Toda EEPROM possui um número aproximado do limite máximo de leitura e escrita até o momento em que se torne inoperante.

Com base em alguns dados, como: número de acessos diários; operações realizadas ao longo do dia; a validade do cartão; podemos chegar a um número mínimo esperado que o chip atenda para evitar re-emissões fora do prazo previsto.

Suponha-se que um usuário com mais acessos utilize o cartão para assinar pelo menos dois e-mails por dia e o use também, ao menos uma vez, para uma identificação completa. Note que talvez isso nem chegue a ocorrer, porém, existirão usuários que farão uso dessa

funcionalidade em uma freqüência muito maior dependendo das suas tarefas e responsabilidades do seu dia-a-dia.

Cada e-mail pode ser assinado com algo em torno de 20 (vinte) ciclos de leitura e escrita, e uma identificação completa pode chegar a algo em torno de 30 (trinta) ciclos de leitura, portanto, ao longo do dia atinge-se cerca de 70 (setenta) ciclos de leitura e escrita.

Com base na informação de que o prazo do cartão é de 10 anos, basta calcular 70 ciclos de L/E x 365 dias x 10 anos = 255.500 ciclos de L/E ao longo da vida normal do cartão. Com isso, pode-de definir cerca de 300.000 ciclos de L/E como requisito mínimo para um cartão com vida útil de 10 anos.

2.5.3. Cartão Mono-Aplicativo x Cartão Multi-Aplicativo

Antes de iniciar o comparativo, é importante ressaltar a diferença entre cartões Multi-Aplicação e cartões Multi-Aplicativo:

- Cartão multi-aplicativo: Significa possuir, carregar ou excluir mais de um aplicativo em um cartão inteligente ao longo de seu tempo de vida normal.
- Cartão multi-aplicação: Significa possuir, conceber ou revogar mais de um propósito a um cartão inteligente ao longo de seu tempo de vida normal não implicando, necessariamente, às suas funcionalidades internas previstas.

2.5.3.1. Cartão Mono-Aplicativo

Existem cartões inteligentes que são designados para carregar um único aplicativo, e estes podem apresentar diversos níveis de sofisticação. O mais simples a ser considerado é um cartão de memória e o mais sofisticado pode realizar algum tipo de processamento que um cartão inteligente multi-aplicativo pode fazer.

Um cartão de memória é aquele que possui um conjunto limitado de instruções que permitem o acesso à memória estática. Na maioria dos casos, esse conjunto de instruções consiste em comandos de leitura e escrita e podem também incluir alguns aspectos de segurança como a criptografia simétrica. Entretanto esse conjunto de instruções não é combinado ao chip para criar um aplicativo executável, ao invés disso, o comando deve ser externamente provido ao chip. Por exemplo, o comando READ BINARY simplesmente

instrui o chip a ler certa área da memória e retornar o que foi lido. Assim como esse comando outros encontrados na ISO 7816-4 podem ser usados.

Cartões inteligentes mono-aplicativo mais complexos permitem executar aplicativos residentes no chip, aos quais permitem um processamento maior de dados assim como sua segurança. Então, esses cartões permitem uma série de instruções combinadas em uma única instrução. Em outras palavras, os cartões são programáveis.

Cartões inteligentes mono-aplicativo se encaixam perfeitamente em diversos negócios. No entanto ainda existem alguns empecilhos. Uma vez fabricado o cartão, é difícil, senão impossível, de alterar o aplicativo no chip. Se um emissor de cartões desejar oferecer diferentes aplicativos aos seus usuários, então um ou mais cartões deverão ser emitidos para o mesmo usuário. Se o projeto não for bem elaborado, o custo para os emissores pode ser muito alto.

2.5.3.2. Cartão Multi-Aplicativo

Cartões inteligentes multi-aplicativo são cartões programáveis que permitem carregar mais de um aplicativo o chip. Cada aplicativo pode ser executado independentemente no chip. Concluindo, um único cartão inteligente pode ser usado para realizar diferentes funcionalidades. Poderia ser possível, por exemplo, ter um único cartão que serve como uma identificação, como cartão bancário e armazenar registros de saúde. Cada um destes aplicativos terá acesso às ferramentas necessárias para prover sua própria segurança.

Aplicativos podem ser carregados e excluídos dos cartões. Essa independência permite usuários e emissores de cartões a alterar essa mistura de aplicativos no chip ao longo do tempo normal de uso. Isso também pode alterar a vida útil do cartão.

Para isso, esses cartões necessitam de um sistema operacional para ajudar a criar um ambiente conhecido dentro do chip ao qual o aplicativo irá operar. Isso também facilita a carga e a exclusão além de outras operações comuns.

Entretanto, cartões multi-aplicativo possuem alguns pontos fracos. O custo de um cartão multi-aplicativo é maior do que os demais. Maior flexibilidade implica em uma maior complexidade, o que significa em uma fase de aprendizado maior.

2.6. ATAQUES AO SMART CARD

Os smart cards permitem guardar informação particular de forma segura. Um exemplo de informação deste tipo é uma chave secreta de criptografia. Para que a segurança seja efetiva, é necessário que exista uma política de segurança adequada ao valor da informação protegida e às ameaças mais prováveis, traduzidas na utilização correta de mecanismos de proteção. No caso dos smart cards, existem mecanismos físicos (implementados por hardware) e mecanismos lógicos (implementados por software).

A designação normalmente dada à segurança de cartões é a resistência a manipulação (tamper-resistance), que significa que o cartão apenas funciona nas condições normais para que foi concebido. Além da resistência também é importante garantir a detecção da manipulação (tamper-evidence), para se saber que a informação protegida foi revelada.

Deste modo, no caso de uma chave criptográfica armazenada no cartão, é possível efetuar a sua revogação o mais rápido possível.

Os ataques ao cartão podem ser invasivos ou não. Um ataque invasivo implica a destruição parcial ou total do cartão. Os ataques não invasivos não destroem o cartão, mas podem deixar rasto de uma outra forma (através do registro de transações efetuadas, por exemplo). Os ataques invasivos são mais caros e necessitam de laboratórios com equipamento especializado. Os ataques não invasivos são mais específicos e escalam melhor, podendo ser aplicados a um grande número de cartões sem um grande aumento do custo.

Uma estratégia típica de ataque é começar por fazer um ataque invasivo para analisar a estrutura física do cartão e identificar vulnerabilidades que depois são exploradas usando ataques não invasivos, de forma mais rápida e barata. Se conseguir detectar o ataque, o cartão pode ignorar os comandos recebidos (e registrar a ocorrência do ataque) ou então autodestruir-se, o que nem sempre é possível por falta de energia ou por o mecanismo de autodestruição ter sido desativado.

Não deve ser nunca superestimada a segurança física de um smart card, pois não existem dispositivos completamente seguros. Todos os cartões podem ser comprometidos, dado um investimento suficiente de conhecimento, tempo, recursos e motivação dos atacantes.

Outra consideração importante é que nem todos os smart cards são igualmente seguros. A implementação de defesas mais eficazes normalmente aumenta os custos de produção, por isso existem muitos modelos apenas com as proteções mais simples.

2.6.1. Mecanismos Físicos de Proteção

Os mecanismos físicos de proteção são relativos ao hardware do cartão e são embutidos durante a sua fabricação. Os mecanismos físicos de proteção podem ser separados a partir de dois tipos de análise: uma estática e uma dinâmica.

2.6.1.1. Análise Estática dos Mecanismos Físicos de Proteção

- Tecnologia do Semicondutor: Para dificultar uma análise física do chip e uma interferência no mesmo, a tecnologia usada na fabricação dos elementos componentes do circuito tem evoluído de forma a produzi-los em um tamanho cada vez menor. A espessura estrutural do chip tem chegado à casa dos micrômetros, aproximando-se muito de seu limite fisicamente mínimo.

- Projeto do Chip: A segurança também envolve o projeto de chips para smart cards. Enquanto o desenho de alguns tipos de chip sejam de fácil acesso, o chip de smart cards é alvo de alto grau de sigilo. Todos os circuitos testes das fábricas são devidamente destruídos e seus projetos guardados a sete chaves, pois pistas como posição das memórias, barramentos, etc. podem ser de grande valia para atacantes incumbidos de descobrir os segredos dos mesmos.

- Barramentos do Chip: Para evitar ataques de ”escuta”pelos barramentos são adicionadas camadas protetoras nos mesmos. Tanto para impedir o acesso como para denunciar uma eventual tentativa. Também são dispostos nas camadas mais baixas dos chips para que uma tentativa de acesso seja responsável pela destruição do circuito, impedindo assim a descoberta dos segredos contidos no chip.

- Projeto da Memória: É projetada para ficar abaixo de uma camada de silicone. Também são equipadas com ion implanted ROMs, em que os dados não são visíveis nem por microscópios óticos, nem por espectros infravermelho ou ultravioleta.

- Blindagem: Para a proteção dos potenciais elétricos emitidos durante a operação existe uma blindagem em todo o circuito. Tem a grande vantagem de ser um detector de intrusão. A blindagem é necessária ao suprimento de voltagem elétrica ao chip, se removida o mesmo simplesmente pára de funcionar. Protege também contra ataques utilizando os FIB (Feixe de Íons Focalizado), mostrado na Figura 2-20.

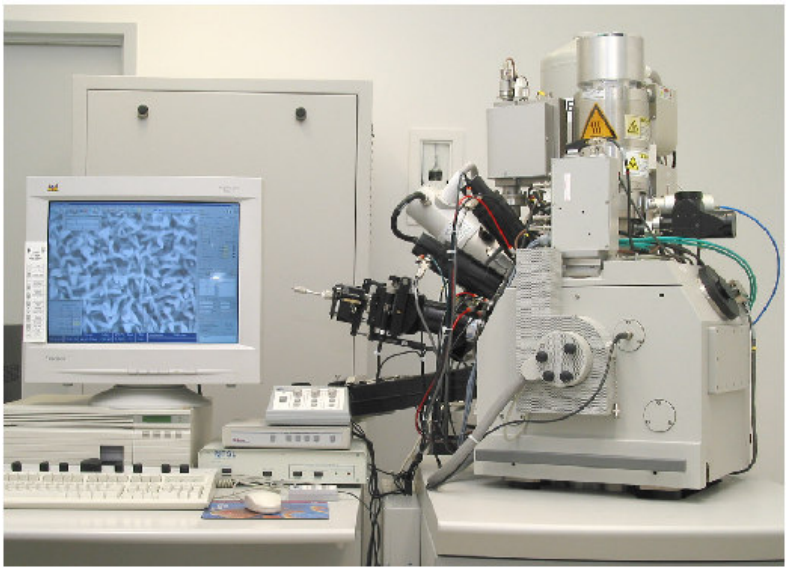


Figura 2-20 - FIB e imagem visualizada em computador

Fonte: National Center For Electron Microscopy [46]

- Embaralhamento da Memória: Esta técnica é muito útil se um atacante porventura conseguir ler o que há escrito na memória. Com a memória embaralhada o atacante precisará da exata informação de embaralhamento para conseguir distinguir alguma informação inteligível. É uma técnica relativamente simples de ser implementada, custando apenas algum espaço adicional na memória para as informações de embaralhamento.

- Criptografia da Memória: Assim como a técnica acima, permite que o atacante ao ler a memória do smart card não consiga interpretá-la. É mais segura que o embaralhamento, mas por outro lado necessita de um pouco mais de processamento, pois a criptografia ocorre em tempo real a cada leitura ou escrita na memória.

2.6.1.2. Análise Dinâmica dos Mecanismos Físicos de Proteção

- Monitoramento da Passivation Layer: A camada em questão protege o circuito contra a oxidação. Tem uma função primordial não só na proteção contra a invasão mas também na detecção da invasão. Em um ataque químico por exemplo, o reagente dissolveria a camada e logo após o faria com o chip, deixando-o assim inutilizado e protegendo os dados confidenciais. Um sensor de capacitância e resistência contido no chip pode detectar a ausência da camada causando também uma interrupção no software, salvaguardando assim de outra forma os dados.

- Controle de Voltagem: Permite que se proteja o smart card de um ataque de geração de faltas. Protege o chip de um ataque do tipo DFA[6]. Uma voltagem acima ou abaixo do esperado pelo processador pode causar erros de cálculo do mesmo. Isso, após várias introduções de erros pode servir para um estudo estatístico dos erros levando facilmente à descoberta de chaves contidas no smart card.

- Monitoramento da Freqüência: Como a taxa de dados é extremamente alta, a sua freqüência de operação é determi-nado por um clock externo, vindo da leitora. Um atacante mal intencionado pode, se não houver esse controle de freqüência, comunicar-se com o smart card em uma freqüência tão baixa que lhe permita fazer um estudo das operações do smart card passo a passo, com isso descobrir segredos sobre o funcionamento do mesmo. O monitoramento da freqüên-cia permite que o smart card não funcione nem em freqüências acima e nem abaixo do esperado (geralmente entre 1MHz e 5MHz).

- Embaralhamento do Barramento: O embaralhamento do baramento além de dificultar ao atacante saber as ligações efetivas entre os componentes do circuito pode também dificultar na atividade de escuta eletromagnética. Este embaralhamento pode ser feito de tal forma que uma linha cancele ou diminua o campo eletromagnético da outra, fazendo da escuta uma missão quase impossível.

Defesas contra o SPA e DPA: A Análise de potência simples, SPA (Simple Power Analysis), é feita simplesmente analisando a potência utilizada para cada instrução realizada pelo processador. A dife-rencial, DPA (Differential Power Analysis), é feita comparando as

[6] Differential Fault Analysis ou, em português, Análise Diferencial de Faltas.

diferen¸cas de potência de cada instrução. São ataques fulminantes e bastante precisos para um chip que não tem a proteção adequada contra eles. Para os chips de hoje em dia esses ataques não são mais eficazes.

Proteções contra esses ataques são: fast voltage regulation, uma regulação rápida de voltagem (feita com o auxílio de um resistor derivativo), o que elimina a diferença de voltagem entre as instruções. A introdução de fontes aleatórias de ruído também evita este ataque, confundindo o atacante, mas prejudica a performance uma vez que necessita de mais energia, elemento crítico em um sistema smart card. Uma introdução de espera aleatória resolve esse problema, confundindo o atacante e não gastando mais energia. Também é útil colocar instruções que consumam quase o mesmo tanto de energia ou várias instruções diferentes que façam o mesmo cálculo, escolhidas aleatoriamente, o que também confundiria o atacante.

2.6.2. Mecanismos Lógicos de Proteção

Os mecanismos lógicos de proteção incluem formas de barrar um atacante por software, fazendo com que seu ataque seja neutralizado através da forma com a qual o software é projetado. Geralmente a proteção lógica vem acompanahda de alguma solução de hardware, ou física.

Como a proteção por software atua de forma mais reativa (espera um novo ataque para descobrir como se proteger dele) elencamos os mesmos através da descrição dos ataques contra os quais eles protegem.

O Falso Smart Card: Este ataque tem por princípio a produção de um circuito que imite o funcionamento de um smart card. A Figura 2-21 demonstra o circuito imitação e é facilmente encontrada na Internet e, inclusive, tem muitas variações:

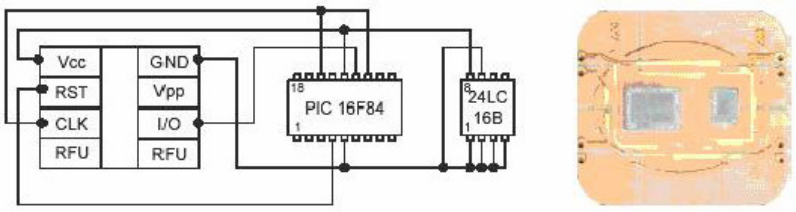


Figura 2-21 - Esquema de um falso Smart Card

Fonte: adaptado de Rankl & Effing [58]

Este circuito serve para um atacante estudar a comunicação entre o terminal e o cartão. Serve também para simular um smart card conseguindo informações de uma base de dados.

Este ataque foi muito útil na época em que os smart cards não eram equipados com as modernas técnicas de criptografia. Hoje este ataque é mais História do que ameaça.

Corte do suprimento de energia: Os comandos do processador podem ser interrompidos durante a sua execução. O fato era que os programadores escreviam todas as instruções na EEPROM e depois as executavam uma a uma. Dessa maneira um atacante poderia cortar a enegia do circuito no momento certo e tirar vantagens disso. A contramedida nesse caso foi a criação de ordens atômicas, isto é, ordens que não po-dem ser divididas. Com isso, ao cortar a energia do circuito, a ordem ou foi completamente executada ou ainda não foi iniciada. Elimina-se, assim, a vantagem do atacante.

Análise da Potência na verificaç˜ao do PIN: Pode-se saber, através de uma pequena variação da voltagem no pino Vcc do smart card, se o resultado de uma comparação entre o PIN fornecido por um usuário, ou atacante, será positivo ou não. Conectando um computador muito rápido e sensível entre a entrada

Vcc do chip e o terminal de leitura, pode-se desligar o fornecimento de energia do chip antes que seu contador interno possa ser acrescido (ao chegar em certo limite do contador as tentativas posteriores são negadas). Com isso um ataque de força bruta seria facilmente efetuado. Duas medidas lógicas são propostas: A primeira é a cada teste incrementar o contador antes do teste e se for o código correto simplesmente decrescê-lo. Isso evita que um corte na energia afete o contador. A segunda é gravar na EEPROM o resultado da comparação antes de externalizar o resultado. Após isso será inútil o corte de energia, uma vez que a EEPROM não é volátil.

Análise do Tempo na verificação do PIN: Como os programadores são geralmente preocupados com o tempo de processamento das suas rotinas eles procuram fazer com que uma instrução seja efetuada da forma mais rápida possível. Com isso, ao comparar um número PIN eles procuravam interromper a rotina assim que se verificasse algum bit que não correspondesse à seqüência correta. Assim, era gerada uma diferença de tempo a cada seqüência diferentes de PIN, o que facilitava, e muito, um ataque por tentativa e erro. Sabendo disso os programadores, para prevenir este tipo de ataque, testam todos os bits do PIN e só

depois retornam o resultado, fazendo, dessa maneira, com que o tempo de comparação seja igual para qualquer PIN.

Criptoalgotitmos sem ruídos: Antigos criptoalgoritmos emitiam diferenças de voltagem e de tempo de execução dependendo da chave e do texto em claro usados. Com isso os atacantes conseguiam, por força bruta, descobrir as chaves criptográficas. Este ataque foi neutralizado com o advento de criptoalgoritmos noise-free (sem ruídos), que mantém o tempo e a potência com diferentes chaves e textos em claro.

Análise Diferencial de Faltas (DFA - Differential Fault Analysis): Afetando o chip com picos de voltagem no momento correto em uma instrução de criptografia, com isso implementando erros nos mesmos, e comparando vários resultados desse procedimento, o atacante pode descobrir a chave secreta de um algoritmo. Este é o princípio do DFA. Não é tão simples como parece e necessita de alguns parâmetros específicos, sendo o principal deles o fato de que o pico de voltagem deve afetar apenas um bit do smart card ou no máximo uma quantidade muito pequena deles. Existem duas formas básicas de, por software, contornar este problema. A primeira é, sempre que se encriptar uma mensagem fazê-la duas vezes e comparar os resultados. Como o erro gerado dificilmente será gerado no mesmo bit, é praticamente impossível provocar erros que gerem a mesma mensagem criptografada. O ponto negativo desta técnica é o consumo excessivo de tempo de processamento necessário para fazê-lo. A outra alternativa é fazer com que o smart card nunca criptografe a mesma mensagem. Para isso a cada mensagem em claro é adicionado um número aleatório antes de criptografar, com isso o atacante poderá colocar a mesma mensagem, mas nunca terá a mesma mensagem criptografada, perdendo assim sua vantagem na comparação dos textos cifrados.

Interrupção do Processador: Estudos comprovaram que ashes concentrados de luz podem interferir no processa-mento de rotinas em um chip. Um smart card, portanto, está vulnerável, além dos pulsos de voltagens, a mais este tipo de interrupção. Um atacante pode, conhecendo a rotina de um programa, por exemplo, alterar um contador de buffer e fazer com que os dados vazem para o terminal. Esses dados podem, inclusive, ser as chaves secretas se estas forem guardadas nos locais indevidos. Meios para se defender desse ataque são vários, desde hardware (detectores de feixes de luz e de picos de voltagem) até software. Como meios lógicos de proteção pode-se contar com uma maior malícia dos programadores desenvolvendo rotinas com o pensamento voltado para a prevenção de uma eventual indução de erro no processamento (como, por exemplo, substituir em uma instrução condicional o

recurso = por um <=, o que no caso de uma contagem afastaria o ataque pela soma de uma contagem a mais em um contador). Vide a rotina como exemplo na Figura 2-22. Esta rotina que pode causar um vazamento de informação pode ser melhorada pela substituição do = por <= na condicional do ponteiro. Outra defesa por software é fazer com que todos os dados a serem gravados na EEPROM sejam encriptados fazendo com que um eventual vazamento dessa informação seja inútil ao atacante.

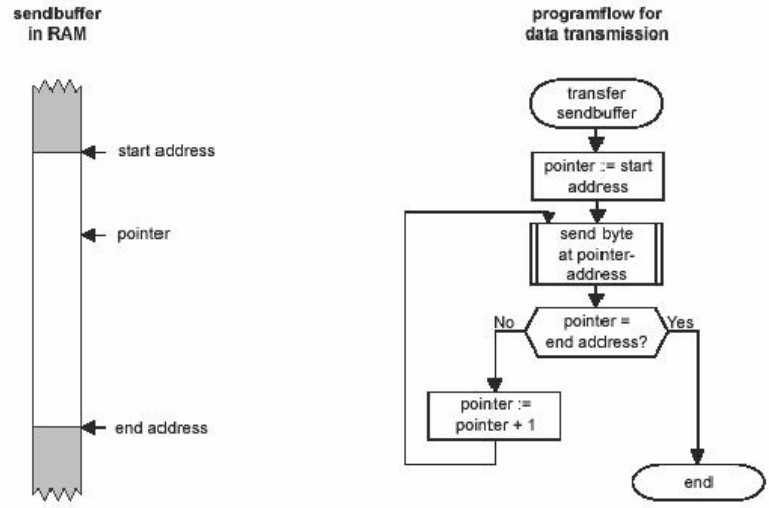


Figura 2-22 - Rotina passível de ataque por interrupção do processador

Fonte: adaptado de Rankl & Effing [58]

Existem ainda outros ataques que não podem ser combatidos apenas com tecnologia, que são a utilização incorreta do cartão e o uso de engenharia social para enganar os utilizadores. Para estes casos é necessário informar os utilizadores, alertando-os para os perigos existentes.

2.7. MERCADO

2.7.1. Smart Cards no Mundo

O número de smart cards tem evoluído bastante em todo o mundo. Como já foi dito, eles têm muitas funções e com isso tem crescido bastante a demanda por este tipo de cartão. Para se ter uma idéia de toda essa evolução, é apresentada a Tabela 2-7, que foi elaborada a partir de estudos de mercado efetuados e divulgados pela Eurosmart (http://eurosmart.com).

Tabela 2-7 - Mercado Mundial de Smart Cards

Cartões por segmento	2003	2004		2005		2006 (Previsão)	
	Processador (MU)*	Memória (MU)	Processador (MU)	Memória (MU)	Processador (MU)	Memória (MU)	Processador (MU)
Telecom	657	710	1050	580	1390	520	1550
Financeiro, varejo e fidelidade	204	35	260	30	336	30	400
Saúde Pública	40	20	45	25	60	25	85
Transporte	12	60	15	73	20	85	25
TV Paga	35	-	55	-	55	-	60
Segurança corporativa	7	10	12	20	25	10	20
Outros	10	10	12	10	22	10	15
Total por tipo 2004	979	845	1469	738	1388	670	2255
Total geral 2004	979	2314		2526		2925	

* Milhões de Unidades

Fonte: Eurosmart [20]

A EuroSmart é uma associação internacional sediada em Bruxelas que se auto-intitula como “a voz da indústria de smart cards para aplicações multi-setor”. A associação é uma organização sem fins lucrativos que tem por objetivo expandir o mercado de smart cards no mundo, desenvolvendo padrões e melhorando continuamente a qualidade e segurança das aplicações.

Os fabricantes de smart cards, de semicondutores, de terminais, de equipamento para integração dos sistemas de smart cards, desenvolvedores e editores de aplicação pesquisam e trabalham em grupos de trabalho dedicados a publicar edições que tangem à segurança, ao marketing e à comunicação.

Com suas atividades, a EuroSmart dá suporte ativamente ao desenvolvimento do comércio de smart cards e age como um catalisador de novas tecnologias e fórum para discussão de temas entre as partes interessadas em smart cards.

A EuroSmart tem como membros: Atmel, Austria Card, Datacard, FNMT, Galitt, Gemalto, GIE Cartes Bancaires, Giesecke & Devrient, Infineon Technology, Ingenico, MasterCard, Moneyline, NedCard, Oberthur Card Systems, Philips Semiconductors, Renesas, Sagem Orga, Samsung, Saqqarah International - Groupe Imprimerie Nationale, Sharp, SST, STMicroelectronics, Wave.

2.7.2. América Latina

A seguir distribuímos duas tabelas produzidas pela Smart card Alliance (http://www.smartcardalliance.org) e divulgadas por Edgar Betts, diretor representante da Smart card Alliance na América Latina, em um documento-convite para participação em sua conferência anual em San Diego (CA - EUA). O documento discorre acerca do mercado de smart cards na América Latina e no Brasil.

A primeira (Tabela 2-8) retrata o número de smart cards no mercado latino americano e o valor desse mercado, incluindo previsões até 2010.

Tabela 2-8 - Mercado Latinoamericano de Smart Cards

	Unidades	Crescimento	Faturamento	Crescimento
Ano	(Milhões de Dólares)	(%)	(Milhões de Dólares)	(%)
2003	35.1		77.4	
2004	84.8	141.7	18601	140.5
2005	136.4	61.0	274.5	47.5
2006	217.2	59.2	420.8	53.3
2007	332.8	53.3	586	39.2
2008	457.4	37.4	764.2	30.4
2009	568.8	24.4	889.6	16.4
2010	667.5	17.4	997.7	12.2

Fonte: Betts [11]

A segunda (Tabela 2-9) retrata as aplicações mais usadas e a sua parcela no universo de smart cards usados na América Latina, assim como sua previsão até 2010:

Tabela 2-9 - Aplicações mais usadas na América Latina

Setor	SIM Card	Bancário	Governo e ID	Controle de Acesso	TV Paga
Ano	(%)	(%)	(%)	(%)	(%)
2003	76.7	22.5	0.3	0.2	0.3
2004	86.4	12.	0.2	0.8	0.2
2005	88.8	9.9	0.2	0.9	0.2
2006	89.9	8.1	0.6	0.9	0.5
2007	90.6	6.9	0.9	0.9	0.7
2008	90.6	6.6	0.8	1.1	0.9
2009	90	6.7	0.9	1.3	1.0
2010	89.2	7.1	1.1	1.5	1.2

Fonte: Betts [11]

O mercado Latino Americano de smart cards foi valorado em 2005 em 274,5 milhões de dólares americanos.

2.7.3. Brasil

O mercado brasileiro é responsável por 45,9% do mercado de smart cards da América Latina, ou seja, 125,9 Milhões de dólares (fonte: Frost & Sullivan/Smart Card Alliance). Se o mercado Latino Americano é equivalente a um total de 136,4 milhões de cartões microprocessados e o Brasil mantém 45,9% do mercado Latino Americano é razoável assumir que existem aproximadamente 62,6 milhões de cartões microprocessados no Brasil. Portanto, a correlação entre smart cards e a população do país é de 33,3%, ou seja, um smart card para cada três brasileiros. Cabe notar que a distribuição destes cartões não é uniforme e algumas pessoas podem possuir mais de um cartão inteligente. (fonte: Frost & Sullivan/Smart Card Alliance).

No gráfico da Figura 2-23, vê-se a distribuição dos Smart Cards no Brasil em relação à sua utilização.

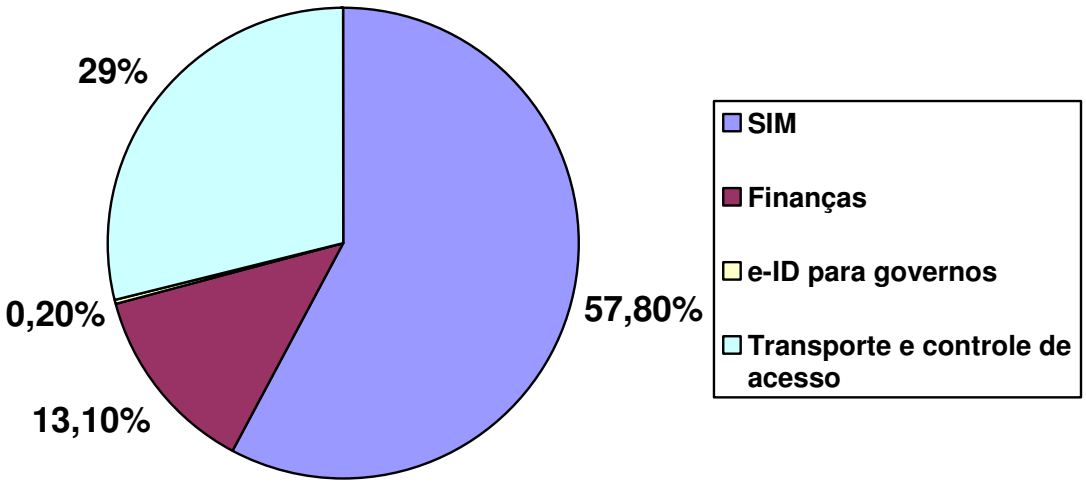


Figura 2-23 - Aplicações de Smart Cards mais usadas no Brasil

Fonte: Betts [11]

O único equipamento homologado no país hoje segundo as normas impostas no regulamento contido na Resolução n o 36 de 21/10/2004 é um leitor/gravador de smart cards

da empresa Perto, a homologação se deu no dia 06 de junho de 2006. A Figura 2-24 e a Figura 2-25 do produto homologado e do selo de conformidade, respectivamente.

Figura 2-24 - Leitor/Gravador de Smart Cards da Perto

Fonte: Perto S\A, 2006 [55]

Figura 2-25 - Selo da ICP-Brasil

Fonte: Infra-Estrutura De Chaves Públicas Brasileira [30]

2.7.4. Fornecedores

A Tabela 2-10 apresenta as maiores empresas envolvidas na fabricação, desenvolvimento e distribuição de smart cards do mundo.

Tabela 2-10 - Maiores empresas envolvidas com Smart Cards por Setor

Setor	Principais Empresas
Fabricantes de cartão	Gemalto, Orga, Obertur e Toshiba
Fabricantes de sistema RFID	Indala, HD Corp, Cubic, Digital Angel, Philips
Fabricantes de terminais de leitura	G&D, KCR, Gemalto, Perto, Bull, Danyl
Fornecedores de Sistemas Operacionais	Gemplus, Bull, G&D, SCS, MCO Group, Sur
Fornecedores de Chip	DuPont, Motorola, Siemens, Hitachi
Fornecedores de circuitos de RFID	Philips, Texas Instrument

Fonte: Adaptado de Allen; Barr, com atualizações [3].

A Tabela 2-11 mostra como o mercado de cartões microprocessados foi dividido nos anos de 2003 e 2004.

Tabela 2-11 - As maiores empresas no mercado de Smart Cards		
Empresa	2003	2004
Axalto (Gemalto em 2004)	25%	22,7%
Gemplus	22%	20,4%
G&D	16%	12,8%
Oberthur Card System	12%	9,3%
Orga	6%	5,2%
Incard	3%	2,8%
Outros	16%	26,8%
Total	100%	100%

Fonte: Gartner [26]

Cabe aqui a observação de que as empresas Gemplus e Axalto agora são uma só, a Gemalto, que abocanha com isso uma boa fatia de mercado.

3. CARTÕES PLÁSTICOS PARA DOCUMENTOS DE IDENTIFICAÇÃO

Nesta seção são apresentadas considerações sobre tipos de materiais utilizados na produção de cartões plásticos destinados a identificação de pessoas. São avaliados os quesitos durabilidade, custo e tipo de impressão dos cartões.

A tecnologia de *smart card* atual está apta a lidar com aplicações destinadas a identificação de pessoas, mas a estrutura física do cartão é crítica – e é necessário encontrar requisitos específicos em termos de durabilidade e segurança, com o uso de novos tipos de materiais plásticos.

A ISO 10373 especifica métodos de teste para muitas características requeridas para atestar a qualidade de um material utilizado no corpo do cartão. Como o chip do cartão é frágil e requer proteção contra estresse mecânico, esses requisitos tornam-se muito importantes para a produção deste tipo de cartão. Vários testes devem ser realizados para assegurar a qualidade do material empregado. Os principais testes são mostrados na Figura 3-1, extraída e traduzida de Rankl e Effing, (2004).

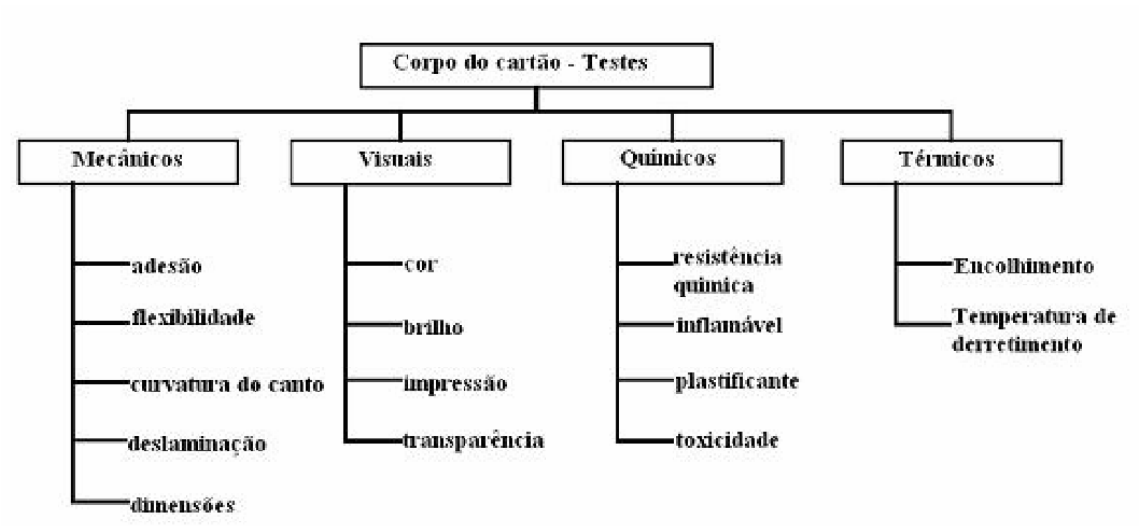


Figura 3-1 - Testes de efetuados no corpo do Smart Card

Fonte: adaptado de Rankl & Effing [58]

3.1. ANÁLISE DE ALTERNATIVAS

Os materiais disponíveis para elaboração de documentos, a partir de projetos baseados em cartões plásticos, laminados ou não e que podem influenciar a escolha do usuário, dependem de vários fatores. Dentre os mais importantes destacam-se como principais critérios de avaliação:

Critérios Técnicos

- Propriedades dos materiais
- Requerimentos de durabilidade
- Requerimentos para segurança

Critérios Econômicos

- Custos de matérias primas
- Custos de produção
- Equipamentos de produção
- Grau de deficiência ou falhas

Critérios Ecológicos

- Produtos recicláveis
- Produtos não poluentes

Algumas vezes os cartões mais adequados para um determinado uso mesclam materiais com características diferentes.

3.2. MATERIAIS E COMPOSIÇÃO DE CARTÕES

Nesta seção apresentamos os tipos mais comuns de materiais e compostos utilizados na concecção de cartões plásticos.

3.2.1. PVC

O PVC (cloreto de polivinila) tem sido o material mais frequentemente utilizado para fabricar cartões de crédito, cartões de identificação e cartões de associados. O grande uso do PVC como material base para cartões plásticos é devido ao fato do baixo custo do material, ser fácil de trabalhar e possuir as propriedades requeridas dos materiais usados nos cartões

plásticos. Porém, as propriedades ambientais do PVC são inapropriadas, e o tratamento de material descartado por incineração é nocivo ao meio ambiente. Uma alternativa seria a reciclagem do PVC que, embora não seja muito comum, é tecnicamente possível.

O PVC é recomendado para aplicações que requerem uma personalização térmica. Impressão térmica produz uma resolução melhor de imagem do que a impressão por jato de tinta e é obrigatória para alguns códigos de barra.

O PVC laminado tem sido o mais usado material para cartões plásticos, desde então ele é o padrão para cartões de transação financeira, como cartões de crédito e débito. Ele é mais durável, mas também mais caro. Ele pode ter impressão térmica por cima de imagens já impressas e alto relevo. A maioria dos cartões de transações, como de crédito ou débito, precisa de uma vida útil longa e por isso são feitos de PVC laminado. A maior parte dos cartões magnéticos e *smart cards* são de PVC laminado.

É um produto que atende todas as exigências normativas de cartões para sistema de identificação, sistema bancário ou private label, estando perfeitamente de acordo com a ISO 7810. Por ser um produto de fácil fabricação seu custo é relativamente baixo além de permitir fácil impressão em processos convencionais, ser laminável em temperaturas médias e permitir personalização por processos termográficos e de alto relevo.

Por outro lado não aceita gravações laser, mas possibilita aplicações hot stamping e tem vida útil de até 4 anos, sem alterar suas características originais, quando manuseado adequadamente. Após descartado pode permanecer no ambiente por muitas décadas. É facilmente reciclável por processos mecânicos e térmicos não sendo necessários aditivos químicos especiais.

Propriedades Mecânicas

- Densidade (DIN 53479, ASTM D792) = 1,36gr/cm³
- Tensão de Alongamento (ISO 527) = 38N/mm²
- Elasticidade até a ruptura (ISO 527) = 120%
- Teste de Impacto (ISO 8526) = 600Kj/m²
- Elasticidade no Teste de Impacto (ISO 8526) = 14%
- Índice de absorção de água (DIN53472, ASTM D70) = 0,05%
- Tensão Superficial (MD) = 38 Dynas

Propriedades Térmicas

- Ponto de Vicat A (ISO 306 A-50) 80°C
- Condições de armazenagem 0 a 35°C, 50 a 75 % URA
- Propriedade Óptica – Material opaco a passagem de luz IR

3.2.2. PVC + ABS

Produto que atende todas as exigências normativas incluindo a ISO 7810 e também recomendado para inserção de chip de contato.

Propriedades Mecânicas

- Densidade (DIN 53460) = 1.23 gr/cm³
- Tensão de Alongamento (ASTM D882, DIN 53455) = 59Mpa
- Elasticidade até a Ruptura (ASTM D882, DIN 53455) = 100%
- Teste de Impacto (ASTMD 1822, DIN 53448) = 500Kj/m²
- Índice de Absorção de água (DIN 53460) = 0,05%
- Tensão Superficial (MD) = 40 Dynas numa face e 37 Dynas na outra face

Propriedades Térmicas

- Ponto de Vicat (ASTM D1525, 1kg Óleo) = 95ºC
- Condições de armazenagem = 0 – 35°C, 50 a 75 % URA
- Propriedade Óptica: Baixa opacidade até a espessura de 399µ
  Média opacidade até a espessura de 400 a 599µ
  Alta opacidade acima de 600µ

3.2.3. Poliéster

Embora haja uma considerável similaridade entre os nomes PETG e PET, estes são materiais diferentes.

O tereftalato de polietileno plano (PET) ou poliéster é mais comumente associado com um material usado na confecção de roupas. Progressivamente, ao longo dos últimos dez anos, o PET vem ganhando aceitação como um material de escolha para garrafas de bebidas.

O PETG, também conhecido como poliéster glicolizado, é usado na produção de cartões. O “G” representa o modificador glicol, que é incorporado para minimizar a fragilidade e o envelhecimento prematuro que ocorre se o tereftalato de polietileno amorfo (APET) não modificado é usado na produção de cartões.

A película PETG é amorfa, significando que as moléculas de poliéster não são alinhadas ou ordenadas dentro do material. O processo de produção do PETG é similar ao do PVC, como resultado PETG possui muitas características similares ao PVC, como resistência a temperatura e durabilidade. Além de ser utilizado em cartões, este poliéster é usado em aplicações onde é requerido o uso de manipulação térmica.

O poliéster é mundialmente conhecido por suas centenas de aplicações. Mais de 930 formas básicas são possíveis de se obter para atingir mais de 90 segmentos de mercado e mais de 140 usos finais específicos.

O poliéster apresentado para fabricação de cartões é um filme biorientado axialmente, branco, opaco com tratamentos térmicos para adesão em duas faces.

Sua obtenção é através de destilação do petróleo (óleo cru), donde se retira a nafta. Empregando-se processo de craqueamento na nafta produz-se o etileno glicol e o ácido tereftálico. O etileno glicol e o ácido tereftálico reagem de forma a produzir o polietileno tereftalato ou PET. Com a eliminação do glicol (PETG) tem-se finalmente o filme de poliéster (PETF).

O polímero assim obtido é processado por extrusoras para produzir a orientação biaxial e, posteriormente, calandrado em forma de filmes.

A orientação biaxial dos filmes PET auxilia na manutenção da estabilidade dimensional do produto final eliminando as possíveis deformações quando em uso.

Os filmes ou lâminas de poliéster são atualmente os principais materiais usados para documentos pessoais de alta segurança, pois pode incrementar requerimentos de durabilidade, tolerâncias térmicas e mecânicas e confiança.

Alguns exemplos de uso do filme de poliéster são: carteiras de identidade, carteiras de habilitação, passaportes e cartões de acesso para áreas de segurança. Isto se deve,

principalmente, pelas suas características de resistência a esforços dinâmicos, resistência térmica superior ao PVC e sua maior vida útil.

Vantagens quando o poliéster for utilizado:

- Durabilidade prolongada
- Altos índices de segurança
- Redução de danos por manuseio inadequado
- Aumento da confiabilidade do produto final
- Redução dos custos por reposição prematura

Propriedades Mecânicas

- Densidade = 150 gr/cc
- Elasticidade até a Ruptura MD (ASTM D882A) = 150%
- Elasticidade até a Ruptura TD (ASTM D882A) = 120%

Propriedades Térmicas

- Propriedade Óptica Transmisssão luminosa (ASTM D1003-77) =7% (152μm)
  5% (254μm)
  2% (307μm)

3.2.4. Policarbonato

Policarbonato (PC) é um plástico da família dos poliésteres aromáticos. Suas principais propriedades são:

- Alta resistência ao impacto;
- Alta transparência: 96%;
- Estabilidade dimensional e térmica;
- Resistência aos raios ultravioleta;
- Usinabilidade;
- Alta temperatura de deflexão;
- Características de isolamento elétrico.

A desvantagem deste material é seu alto custo comparado ao de outros materiais. Podem ser atingidos incrementos de durabilidade, altas tolerâncias térmicas e mecânicas e maior grau de confiança superior além do material permitir gravações a laser.

Entretanto há algumas dificuldades de laminação, exigindo temperaturas e tempos de ciclos mais elevados. O processo de corte é dificultado em função da alta dureza dos materiais laminados, provocando, em casos eventuais, deformações e criação de irregularidades visíveis nas bordas. O PC apresenta características de longa vida útil nas propriedades mecânicas e térmicas, porém tem deficiências com agentes químicos que podem vir a interferir em sua performance. Adicionalmente, a sua alta rigidez pode ocasionalmente propiciar empenamento ou deformações permanentes.

Propriedades Mecânicas

- Densidade (ISO 1183) = 1200 Kg/m³
- Elasticidade até a Ruptura (ISO 527-1,-3) = >100%
- Índice de Absorção de água (ISO 62) = 0,2%

Propriedades Térmicas

- Propriedade Óptica Transmissão luminosa (ISO 13468-2) = >80%

3.2.5. Análise Comparativa

A Tabela 3-1 comparativa a seguir apresenta uma visão geral sobre as principais propriedades dos materiais possíveis de emprego para a fabricação de um cartão inteligente.

Tabela 3-1 - Comparação entre matérias-primas

Propriedades	PVC	ABS	PC	PETF	Poliéster Amorfo	PETG
Temperatura Máxima (°C)	75-90	75-100	160	200-230	65-75	60-85
Temperatura Mínima (°C)	-20	-40	-100	-70		
Propriedades Mecânicas	Baixa durabilidade, máximo de 2-3 anos com qualidade constante	Alta resistência mecânica	Alta estabilidade mecânica, alta durabilidade com alta estabilidade, baixa resistência a riscos e a solventes	Alta estabilidade mecânica, alta durabilidade com consistente alta estabilidade	Baixa durabilidade, torna-se quebradiço com o tempo	Similar ao PVC com menor resistência a temperaturas

Laminação	Boa laminação	Pode ser laminado	Necessita de PE ou adesivo	O PETF coextrudado funde-se ao PVC, PET e PETG	Boa laminação	Boa laminação
Impressão	Fácil impressão e média definição de impressão	Fácil impressão após pré-tratamento	Necessita tintas especiais	Impressão pode ser realizada com tintas UV ou a base de água e excelente definição de impressão	Boa impressão	Boa impressão

3.2.6. Cartões com composição de materiais

Existem, ainda, cartões que podem ser produzidos a partir da mistura de materiais, como mostra a Tabela 3-2.

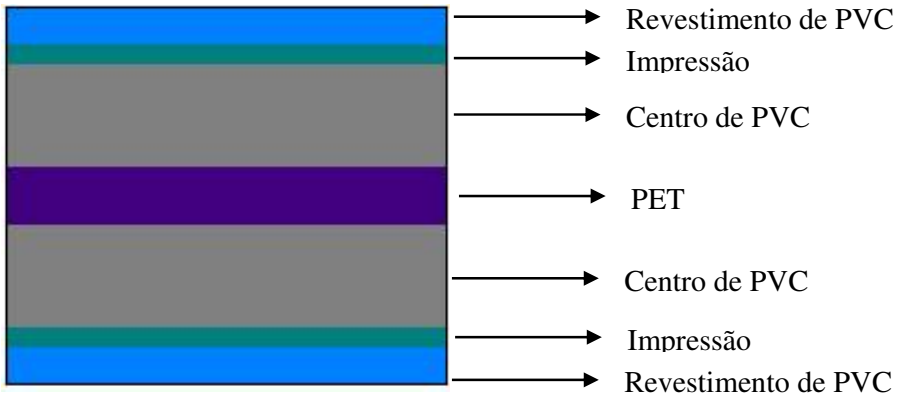
Tabela 3-2 – Tipos de cartões mistos.

Material	Cartão Tipo I	Cartão Tipo II
Película de PET orientado de alta resistência branco opaco	20%	40%
Película de cloreto de polivinila branco opaco	60%	40%
Película de cloreto de polivinila transparente *laser engraving*	20%	20%
Vida útil prevista	Até 7 anos	Até 11 anos

Ambas as estruturas devem ser complementadas com tintas de impressão de alta qualidade, vernizes de segurança e laminados em condições específicas.

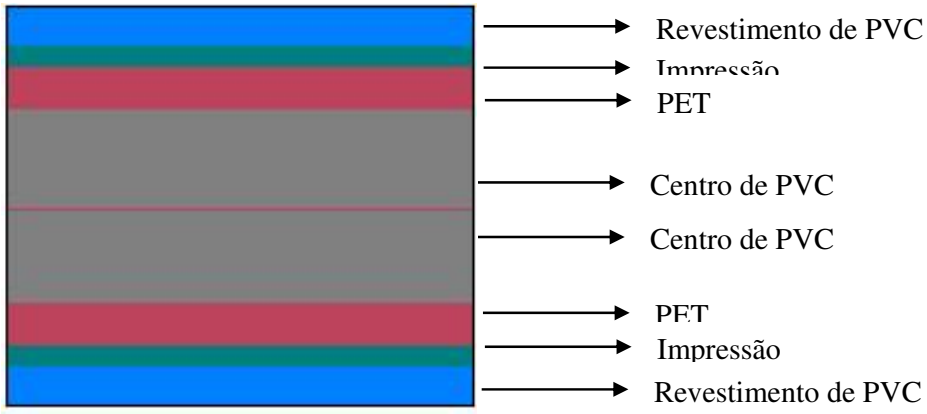
Estes produtos devem ser elaborados conforme norma ISA 7810, formato CR80 e recomendados para documentos de identificação que não prevêem substituição freqüente.

As Figura 3-2 e Figura 3-3 seguintes ilustram esses dois tipos de cartões.



- Simples, estrutura fácil de contruir;
- Acrescido de performance mecânica e térmica versus cartões de PVC padrão;
- Impressão é feita no PVC convencional.

Figura 3-2 - Cartão Tipo I: 20% PET, Branco.



- Estrutura mais forte do que a dos cartões Tipo I e de PVC padrão;
- Impressão é feita no PET.

Figura 3-3 - Cartão Tipo II: 40% PET, Branco.

Fonte: adaptado de www.seiproducts.com

Testes empíricos também demonstram a diferença nas propriedades mecânicas de cartões desenvolvidos com diferentes composições como podemos observar na Tabela 3-3 a seguir.

Tabela 3-3 – Comparação empírica de resistência mecânica

Composição dos Cartões	Ciclos de Flexão	Ciclos de Torção	Resultados
PETG/PETF 300 microns de PETF e 500 microns de PETG	200.000	250.000	Sem danos, chip intacto.
PVC/PETF 100 microns de PETF e 700 microns de PVC	200.000	190.000	Flexão: fraturas visíveis em 150.000 ciclos, porém teste foi completado. Torção: rachaduras iniciaram em 160.000 ciclos com quebra em 190.000 ciclos.
PVC	5 a 30.000	5 a 30.000	95% foram danificados na região do implante do chip.

4. SEGURANÇA DE DOCUMENTOS DE IDENTIFICAÇÃO

Segurança de documentos é um processo contínuo de projeto de sistemas usando experiência, recursos e tecnologia de segurança no esforço de proteger a informação contida no documento e o valor que essa informação representa. A natureza dinâmica tanto das atividades ilegais quanto da tecnologia exige esse esforço contínuo.

A idéia de que o projeto de segurança de documentos incorpora tecnologia ou itens de segurança no esforço de proteger o documento de falsificação ou alteração é errada. Um projeto de segurança adequado começa com a investigação inicial para determinar a fonte dos problemas, identificando, por exemplo, quem está envolvido na produção de falsificações, onde são produzidos, quais são os tipos de tecnologia de impressão, técnicas de falsificação e golpes que são usados.

A seguir, o projeto de segurança inclui outros elementos tais como segurança física, auditorias internas, rastreamento da produção, autenticação e restrições visuais para auxiliar a proteção do documento. Nesse momento entram especialistas das áreas legais, financeira, de produção, vendas e auditoria interna que devem ser envolvidos no projeto. Por fim, o projeto físico incorpora tecnologia de segurança de impressão para atingir os objetivos estabelecidos, levando-se em consideração a relação custo-benefício. Esses objetivos devem incluir o rastreamento tanto do documento quanto do seu uso, além dos custos contínuos de monitoramento, patrulhamento, investigação e litígio no sentido de se tornar o mais eficiente possível.

O avanço e a popularização das várias tecnologias aplicadas ao projeto e à produção de documentos seguros fazem a tarefa de manter as ameaças ao menor nível possível, uma tarefa ainda mais complexa. Uma arquitetura planejada de componentes de segurança devem ser implementada continuamente no sentido de se colocar sempre à frente dos falsificadores e de outras ameaças. Um bom exemplo desse conceito pode ser observado nas ações tomadas pelo Governo dos EUA, que vem atualizando a arquitetura e os componentes de segurança de sua moeda a cada 5 anos [60].

Qualquer discussão a respeito de fraude de documentos deve contemplar a tarefa de identificar as atuais ameaças à segurança do documento e as possíveis ameaças no futuro.

Uma coisa é fato: Todos os documentos que possuam valor ou tenham potencial de criar valor estão sujeitos a fraudes.

4.1. VISÃO GERAL – TERMINOLOGIA

Uma introdução aos termos e conceitos inerentes a segurança de documentos se faz necessária nesta seção.

4.1.1. Proteção dos originais

A necessidade de proteger o acesso a documentos genuínos de valor é a primeira e principal tarefa. Inúmeros casos de fraude são conseqüência de práticas negligentes no que diz respeito ao acesso a documentos genuínos ou aos equipamentos de produção de documentos. A melhor maneira de praticar uma fraude com um documento é ter um documento original nas mãos. Procedimentos frágeis para garantir a segurança servem como um convite ao crime.

Parte da tarefa de proteger documentos originais é a necessidade de um programa efetivo de auditoria e medidas adequadas de segurança. Todos os fornecedores envolvidos devem possuir instalações seguras e processos seguros para a produção de qualquer componente usado na produção de documentos seguros. O processo deve ser percebido como uma cadeia, onde o elo mais frágil é aquele mais provável de ser o alvo de alguém interessado em fraudar um documento.

O processo de auditoria deve permitir o conhecimento de itens perdidos ou roubados. Deve ser prática comum separar as responsabilidades dentro de uma organização. Dessa forma, pode ser considerado negligente ter a documentação, a assinatura e os processos de conferência de forma individualizada. Em alguns casos, os patrões de uma organização podem ser responsabilizados pelos atos de seus funcionários, onde a falha na separação de responsabilidades contribui para o problema.

As pessoas envolvidas na produção, armazenamento ou transporte de documento de valor devem ter um cuidado razoável para proteger estes itens de um acesso não autorizado. Uma pessoa ou empresa que possua matrizes, filmes ou trabalhe no processamento de materiais ou bens acabados que pertençam a terceiros devem tomar um cuidado razoável para que esses materiais estejam seguros contra um acesso não autorizado, podendo ser responsabilizados por perdas resultantes de um acesso não autorizado.

Por fim, no que se trata de documentos originais, é importante conduzir revisões periódicas das medidas de segurança. Criminosos gastam tempo para entender as vulnerabilidades e atacar os pontos fracos. Por exemplo, se as medidas de segurança são implementadas para itens de um certo valor ou acima, cedo ou tarde haverão fraudes na faixa abaixo do valor especificado. Portanto, conclui-se que se tem muito a perder divulgando inadvertidamente certos detalhes da operação de segurança.

4.1.2. Falsificação

A reprodução não autorizada de um documento para fins ilegais é uma grande ameaça. Essa reprodução pode se dar por digitalização, cópia, ou impressões ilegais.

Softwares de editoração eletrônica disponibilizam alta capacidade para a criação de documentos quase similares aos originais. Os custos de digitalização, computadores, impressoras não são barreiras intransponíveis para os criminosos. Com pouco investimento, um criminoso, digitaliza um documento, e manipula sua informação na tentativa de cometer uma fraude.

Copiadoras coloridas e impressoras de cartões evoluíram tanto a ponto de se tornarem acessíveis a quase todos. Na são necessárias grandes habilidades para operar uma copiadora ou uma impressora de cartões, tornando-se a mais simples ameaça na fraude de um documento. Cópias colorida produzem réplicas muitas vezes convincentes e isso abre portas para os criminosos que não possuam muitos recursos.

O acesso, fora do horário comercial, a empresas legítimas de impressão, pode contribuir para a confecção de documentos falsos. Frequentemente, sabe-se do envolvimento involuntário de empresas em operações de falsificação. Operações dessa natureza requerem maior investimento e expertise do que outros métodos de falsificação.

4.1.3. Adulteração

A alteração de um documento para práticas ilícitas é também uma grande preocupação. A adequada proteção dos dados personalizados é um dos itens mais importantes a ser considerado. Sem a proteção adequada desses dados através de tecnologias de impressão em camadas, criptografia e outras, os dados podem ser facilmente modificados.

Um criminoso pode alterar o nome ou uma data em um documento simplesmente apagando ou raspando o dado e substituindo. Utilizando as técnicas adequadas, as chances de obter êxito são muito grandes.

4.1.4. Detecção de fraudes

Existem dois aspectos fundamentais na detecção de fraudes: a detecção de um documento falso e a autenticação de um documento original. Ambos são importantes no combate a fraudes e todos os esforços devem ser feitos para encontrar uma gama de itens que proporcionem máxima proteção.

A detecção de um documento falso significa que um crime já foi cometido. O documento foi duplicado ou alterado. Alguns itens são projetados para dificultar a duplicação de um documento através de inspeção visual pelos responsáveis para tal tarefa, que deve ser facilmente cumprida em quaisquer condições. O objetivo é criar informação visível que permita uma pessoa não treinada validar o documento.

4.1.5. Tecnologias de segurança

Fraudar um documento, algumas décadas atrás, era apenas uma questão de trocar uma foto com um estilete, por exemplo. Não se requer muita habilidade para isso e a fraude frequentemente alcançava resultados.

Hoje, com computadores potentes e softwares inteligentes disponíveis, a falsificação se tornou mais contundente e acessível. O fácil acesso a essa tecnologia tem contribuído para o constante crescimento de atividades criminais com o objetivo de falsificar documentos.

Para garantir a eficácia na segurança de um documento, devem-se levar em consideração os seguintes elementos:

- Fácil reconhecimento: espera-se que o documento seja fácilmente autenticado a olho nu.

- Resistência a fraudes e falsificações : o documento deve possuir itens de segurança suficientes para dificultar e até mesmo impedir as práticas mais comuns de fraudes tais como a adulteração mecânica ou química, reproduções, imitações ou mesmo a reemissão de um documento original.

- Evidenciar fraudes : A tecnologia utilizada na confecção do documento deve permitir que as tentativas de fraude tornem-se evidentes e inutilizem o documento.

- Custo e dificuldade para cometer uma fraude

Grande parte das tecnologias de segurança utilizadas em documentos de papel serve para a confecção de documentos plásticos tais como marcas d`água e fibras UV. Além disso, existe uma gama muito grande de tecnologias de segurança empregadas em cartões plásticos, um extenso portfolio de mais de 200 tecnologias, das quais algumas devem ser escolhidas e combinadas conforme a aplicação desejada.

Estas tecnologias podem ser categorizadas da seguinte forma :

- Impressões de segurança: Fixas e variáveis

- Materiais camuflados entre as camadas dos cartões

- Dispositivos ópticamente variáveis

- Tintas de segurança: Camufladas, Opticamente variáveis, etc

- Segurança de dados: Criptografia embutida nas imagens

Existe uma gama de itens que são projetados para deter ameaças específicas. Como muitos sistemas de segurança, a estratégia é aperfeiçoar o nível de proteção e selecionar alguns itens complementares entre si.

4.1.6. Autenticação

Para uma autenticação completa e efetiva deve-se buscar a combinação da autenticação de três elementos: O documento, seu portador e os dados, conforme a Figura 4-1:

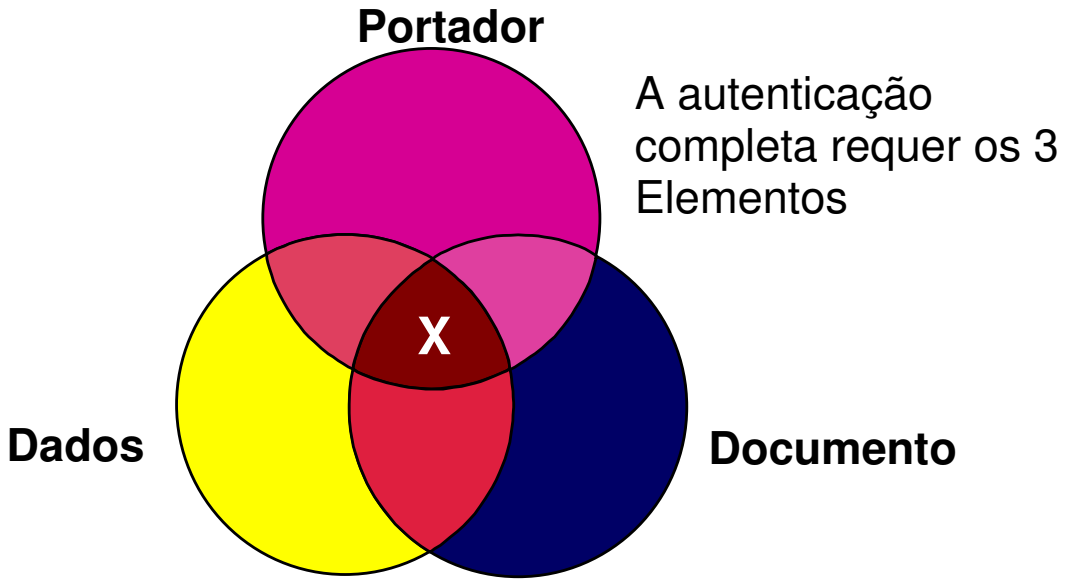


Figura 4-1 – Autenticação Completa

4.1.6.1. Autenticação do documento

A autenticação de um documento original é uma tarefa difícil quando não se sabe como ele deve parecer. Portanto, o objetivo é criar informação visível que permita sua autenticação, a qual contenha itens facilmente identificáveis por um examinador não treinado.

4.1.6.2. Autenticação dos dados e do portador do cartão

O processo onde os dados armazenados no cartão são comparados com outros dados supostamente corretos é chamado de autenticação do portador do cartão. Os dados armazenados no cartão apresentam-se em diferentes formatos, tais como, informações de texto, fotografia, assinatura, biometria e senha (PIN). Estas informações podem ser armazenadas em diferentes mídias, tais como, tarja magnética, código de barras, smart cards e cartões ópticos. As informações, normalmente, são adicionadas ao cartão quando da sua expedição em local seguro. No caso de smart cards e cartões ópticos ainda existe a opção de uma atualização posterior dos dados. Os dados armazenados ainda podem ser protegidos por criptografia.

Seguem alguns métodos de autenticação do portador são descritos a seguir :

- Fotografia: o método mais utilizado na autenticação do portador do cartão. Uma foto colorida pode facilmente identificar o portator confirmando a

autenticidade do documento tanto por pessoas como por máquinas. Nesse último caso é requerido a utilização de smart cards ou cartões ópticos.

- Texto impresso: A maneira mais fácil de autenticar o portador. Basta comparar as informações impressas neste documento com as informações de um outro documento do portador ou com os dados gravados numa tarja magnética, código de barras e smart card. No último caso, a utilização de uma leitora de cartões torna-se obrigatória.

- Assinatura: A assinatura é outra forma de verificação de informação impressa no cartão., apesar da dificuldade de percepção no cause de fraudes.

- Código de barras bidimensional: Suporta mais informação do que um código de barras comum e do que a tarja magnética. Uma significante quantidade de dados pode ser facilmente utilizada para a autenticação do portador. É possível, por exemplo, guardar as minúcias da impressão digital junto com informações biográficas no código de barras bidimensional e comparar essas informações com a digital colhida do portador. A característica única das digitais pode ser um elemento muito importante no combate a fraudes.

É importante ressaltar que a verificação dos dados do portador feita por pessoas depende do comprometimento e treinamento para diminuir a possibilidade de fraudes. Portanto, para uma maior segurança em projetos de larga escala, recomenda-se a utilização de dados que possam ser verificados por máquinas.

4.1.7. Separação em camadas

Separação em camadas é uma estratégia de um sistema de proteções trabalhando em conjunto para prover maior segurança. Uma boa analogia para se entender o conceito de separação em camadas pode ser ilustrado na segurança de uma casa. A camada mais básica seria ter em uma casa portas e janelas que possam ser fechadas e trancadas. A próxima camada pode ser representada pela instalação de *timers* na iluminação para parecer que a casa está ocupada. Outras camadas podem ser representadas pela inclusão de cadeados, cercas, cachorro, sistemas de alarme e assim por diante. Essa estratégia visa levar o criminoso a procurar locais menos seguros como alvo, desistindo do alvo inicial.

Em segurança de documentos, o correto é combinar itens de segurança complementares que estão no documento, sobre o documento ou aplicado ao documento. Essa combinação pode ser composta por itens ocultos, que possam revelar fraude e itens óbvios para a autenticação do documento. A necessidade de equilibrar a habilidade de detecção de fraude com a facilidade de autenticação do documento é criticamente importante. Há valor agregado em cada item.

4.1.8. Considerações em Projetos de Segurança

Poucos projetos de segurança duram mais que poucos anos. A tecnologia avança rapidamente e criminosos rapidamente tem acesso a produtos comerciais capazes de gerar cópias razoáveis. Portanto, a escolha dos itens de segurança deve incorporar a antecipação de ameaças bem como as ameaças atuais de falsificação e adulteração.

Alguns itens de segurança devem ser incluídos para cada nível de inspeção. Muitos itens, por sua natureza, oferecem múltiplos níveis de proteção. Informações para o público geral e treinamento para os examinadores de primeiro nível, garantindo o comprometimento de todos. Isso também é válido para examinadores de segundo nível.

Itens de terceiro nível são mais utilizados em investigações. Quando um documento chega para a análise em um laboratório, provavelmente um crime já foi cometido, uma vez que a falsificação tornou-se evidente em níveis anteriores. A análise forense pode perceber excelentes falsificações com precisão.

Alguns itens devem ser guardados como reserva. Uma vez que os itens iniciais são comprometidos, os itens reservas podem ser anunciados. Enquanto isso, a próxima geração pode estar sendo desenvolvida. Ao mesmo tempo torna-se útil a inclusão de itens de segurança que ainda não estão em uso na autenticação do documento, forçando o criminoso gastar tempo e recursos tentando copiar estes itens, aumentando as barreiras à fraude, e podendo deixar rastros para a investigação.

4.1.9. Produção de documentos e materiais

A utilização de substratos plásticos na produção de documentos de alta confiabilidade oferece além de maior durabilidade, um nível de segurança comparável e potencialmente maior que o nível de segurança inerente aos tradicionais documentos de papel. É importante enfatizar que a mera utilização de itens de segurança em cartões plásticos não garante a

segurança do documento. O Projeto de padrões de uso é um elemento chave na elaboração de um documento. Um cartão plástico possui múltiplas camadas para inserir itens de segurança que podem ser tanto detectados pelo olho humano com por máquinas. A maioria dos processos de impressão de segurança é consistente entre papel e plástico, entretanto a aplicação de tintas em plástico requer conhecimentos e técnicas especialistas, cujo acesso não é tão fácil quanto no caso do papel, bem mais acessível no mercado.

Em qualquer documento, o nível de segurança atingido não é função de um único item de segurança, mas da combinação de diversos itens e processos. Segurança física e auditoria no local de produção do documento são ambos importantes.

4.1.10. Produção de Cartões Plásticos

Um cartão plástico padrão deve ser produzido para atender ou exceder as recomendações dos padrões ISO 7810, ISO 7816-1 e ISO 7816-2.

Todos os cartões devem ser produzidos em instalações de alta segurança licenciadas para a produção de cartões de crédito. Os requerimentos impostos por emissores de cartões de crédito garantem que as instalações licenciadas ofereçam os requerimentos de segurança necessários. Os procedimentos de controle e auditoria devem ser regulados e monitorados por toda a planta de produção. Cada departamento, desde a produção gráfica até o despacho deve ter a qualidade, auditoria e segurança constantemente checados.

Litografia em *offset* e *silkscreen* são utilizados como processos de impressão na produção dos cartões. Além disso, o processo de laminação que finaliza a produção, expõe o cartão a níveis de temperatura e pressão projetados para unir todos os elementos de sua construção.

As tintas utilizadas devem possuir alta performance e resistência às condições ambientais tais como a luz do sol, calor, humidade, etc.

4.2. ITENS DE SEGURANÇA DE IMPRESSÃO INCORPORADOS NA FABRICAÇÃO DO CARTÃO PLÁSTICO

Documentos seguros devem ser validados como originais através de mecanismos de segurança complementares em 3 níveis de inspeção, conforme mostrado na Figura 4-2:

- Nível 1 – Exame superficial, sem a utilização de ferramentas, de fácil identificação visual ou tátil para rápida inspeção.
- Nível 2 – Identificação com dispositivos de visualização simples tais como lentes de aumento, luz UV ou equipamentos de leitura.
- Nível 3 – Inspeção através de dispositivos especiais conduzidas por especialistas cujo exame detalhado permite uma avaliação mais profunda da autenticidade do documento.

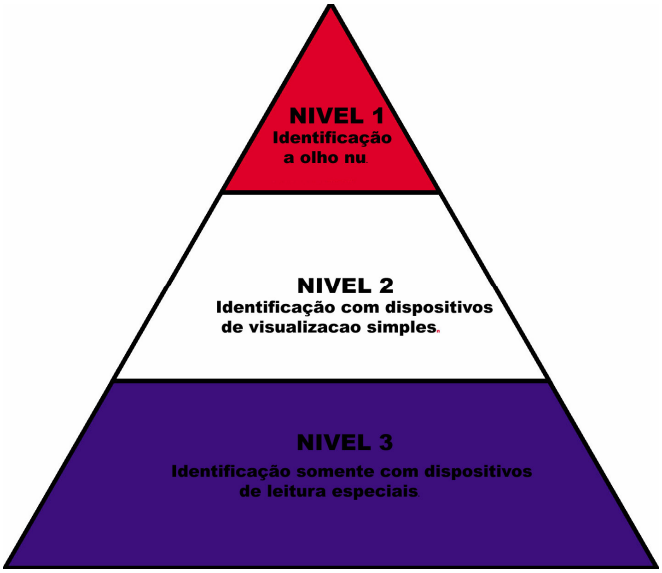


Figura 4-2 - Níveis de Segurança de um Documento

4.2.1. Nível 1: Inspeção a olho nu

A maioria dos componentes de segurança em documentos impressos são ópticos. Isso significa que a inspeção é feita utilizando elementos visuais para a validação de um documento. O primeiro nível de inspeção (superficial, a olho nú) é uma parte importante nas medidas efetivas de segurança em um documento.

O primeiro nível de segurança pode ser implementado de três maneiras: Itens de segurança podem ser embutidos no papel, inclusos na arte do documento ou aplicados ao documento utilizando um dispositivo de imagem variável por difração óptica (DOVID –

Diffractive Optically Variable Image Device) ou uma estrutura de imagem segura por interferência (ISIS – Interference Security Image Structure). Itens de segurança embutidos são utilizados na maioria das cédulas de dinheiro mundo afora. Utilizadas desde o século 14, as marcas d'água criadas pela variação da densidade do papel para criar uma imagem que não pode ser removida sem destruir a cédula ainda são utilizadas até os dias de hoje. Fibras fluorescentes visíveis através de luz ultravioletas também são adicionadas às cédulas.

4.2.1.1. Itens de segurança relacionados com o projeto do leiaute do cartão

Itens de segurança relacionados com o projeto do leiaute do cartão derivados da execução de impressão em equipamento de offset de alta resolução. Derivados de métodos clássicos de segurança em papel, que estão sob constante ataque pelo uso de impressoras e copiadoras digitais. Se propriamente inspecionados e definidos podem ser utilizados com eficiência.

- Linha Fina / Impressão Guilloche: Consistem na impressão de linhas finas paralelas e, geralmente, em ondas com espaços em branco em determinadas posições que torna praticamente impossível a cópia em simples copiadoras, mesmo coloridas, como mostrado na Figura 4-3.

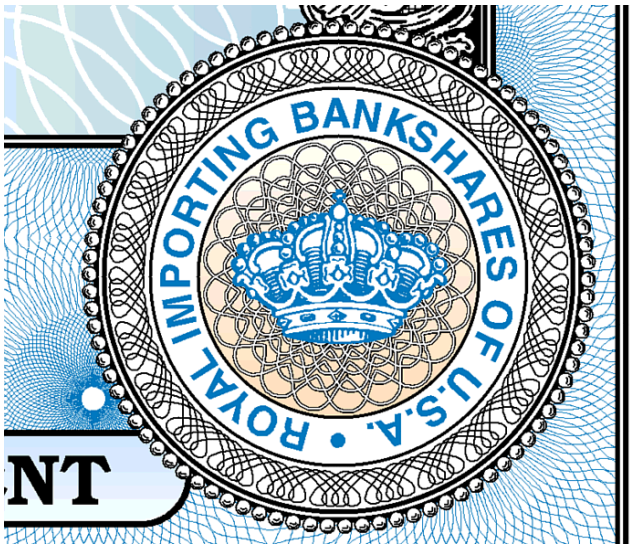


Figura 4-3 - Impressão Guilloche
Fonte: www.amgraf.com

- Impressão em arco-íris (“Rainbow”): Consiste em impressão de duas cores misturando-se suavemente, convergindo do claro para o escuro. Requer o uso de equipamento de impressão especial. A Figura 4-4 mostra exemplos desta técnica.

Figura 4-4- Impressão em Arco-íris
Fonte: www.codeinc.com

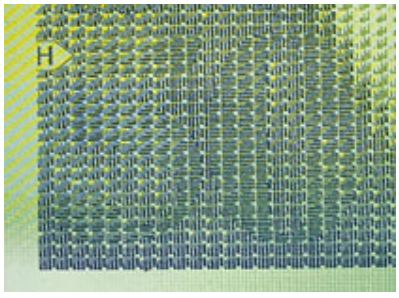
- Modulação de Imagem (padrões de Moiré): Consiste na impressão de armadilhas criadas através da modulação da freqüência ou amplitude das linhas que como resultado gera um padrão visível quando o documento é “escaneado” e/ou copiado (por exemplo, palavras ocultas tais como “invalido” ou “copia” são reveladas quando o documento é submetido a copia ou digitalização). Estes padrões são produzidos pelo uso de programas de desenho altamente sofisticados.

- Modulação de tela: em freqüência, ângulo ou tamanho de ponto (dot size).

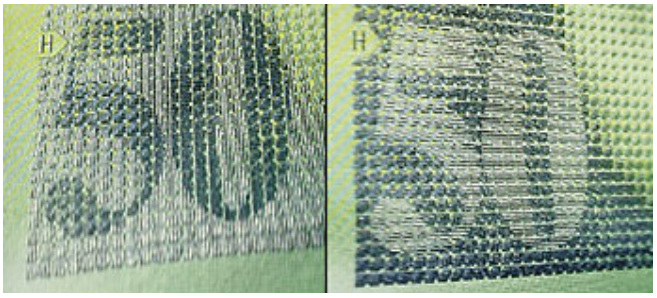
- Erros Deliberados: Consiste em imprimir erros deliberadamente, de maneira conhecida apenas pelas autoridades competentes, tal como mostrado na Figura 4-5.

Figura 4-5 – Erros deliberados
Fonte: www.emergentchaos.com

- Litografia: Elementos de relevo tátil para verificação de segurança.
- Desenhos a partir de linhas de fractais, distorções curvas e efeitos 3D.
- Textos e imagens latentes por impressão intaglio: Provavelmente o mais antigo exemplo de impressão como um dispositivo contra falsificações seja a impressão intaglio. O processo envolve impressão de documentos a elevada pressão para criar um relevo, uma estrutura tátil de tinta e papel.A impressão Intaglio pode ser usada para criar imagens latentes, com linhas horizontais no fundo criando a estrutura e linhas verticais superpostas. Quando vistos de um certo ângulo, as linhas da frente fazem sombra em relação ao fundo, trazendo a figura em destaque conforme a Figura 4-6.



(A)



(B)

(A) Uma imagem latente impressa em intaglio, fotografada sobre um ângulo normal da nova nota de 50 Francos Suíços.
(B) A mesma imagem latente impressa em Intaglio fotografada sob ângulo agudo resultando no contraste entre frente e fundo.

Figura 4-6 – Impressão Intaglio
Fonte: www.banknotes.com

4.2.1.2. Impressão com tintas especiais de segurança visíveis a olho nú

- Cores Customizadas, fora do padrão: O uso dessas tintas torna difícil a cópia/reprodução devido a dificuldade de obtê-las no mercado convencional.

- Tintas metalizadas ou peroladas: feitas a partir de Pigmentos metálicos. Tintas metálicas produzem um efeito brilhante quando impressas em comparação ao efeito opaco de outras tintas. São usadas, geralmente, em grandes áreas de cores sólidas para maximizar o efeito. O uso de tintas metalizadas ou peroladas impede a cópia por modernas copiadoras coloridas ou reproduzidas por scanners para reimpressão.

- Tintas variáveis opticamente (OVI – Optical Variable Ink): Tintas variáveis oticamente podem ser incorporadas aos desenhos dos cartões para criar uma mudança visual de cor (exemplo, verde para roxo, dourado para verde etc.) dependendo do ângulo da luz incidente na visualização do cartão. Este material consiste de tinta transparente sem cor contendo avançadas estruturas multicamadas microscópicas. A disponibilidade deste tipo de tinta é altamente restrita dificultando o uso fraudulento

- Tintas "iridescent": tinta numismática que reage conforme o ângulo de visão.

Figura 4-7 – Tintas visíveis variáveis opticamente
Fonte: www.currencyproducts.com

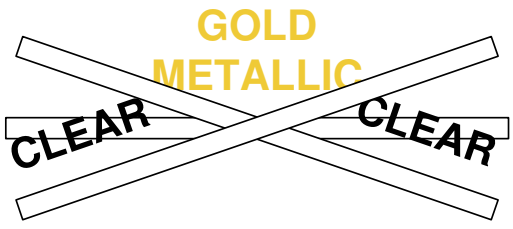


Figura 4-8 – Variação de imagem colorida metálica

Fonte: www.currencyproducts.com

4.2.1.3. Dispositivos Opticamente Variáveis (OVD - Optical Variable Devices)

Frequentemente referidas como um iten de segurança complementar, folhas metálicas podem ser adicionadas a um documento impresso para garantir a autenticidade. Tais dispositivos são geralmente adicionados aos cartões através de sistema "Hot Stamping". Estes dispositivos possuem como característica principal a mudança de aparência conforme o ângulo de visão. Tais dispositivos não podem ser copiados e/ou "scaneados" para reprodução em impressora digital.

A exclusividade da arte impressa no documento gerada por computador, cuja imagem tem 1.690.000 pixels por polegada quadrada e cada pixel possui 1 de 260 variações refrativas, tornam os dispositivos opticamente variáveis tão complexos quanto seguros.

A elaboração de imagens com dispositivos opticamente variáveis começa com a criação da arte a ser impressa, cujas imagens são originadas através de laser e da recombinação iterativa da imagem, moldando a imagem com coberturas proprietárias e ainda metalizando o relevo com metais refrativos e customizando para as especificações do cliente.

Dispositivos iridescentes ou furta-cor: Reage conforme o ângulo de visão.

ISIS (light Interference Security Image Structures)

Tecnologias com estruturas não-difrativas.

- Retro reflexivo (3M Confirm™): É um item camuflado de segurança que inclui um padrão de fundo retro reflexivo com segurança. Na qualidade de item camuflado, o padrão de fundo retro reflexivo não é visível na luz ambiente. Porém, quando vista sob uma luz focada, reflete um brilho que oculta fotos e dados permitindo verificar a integridade do padrão de fundo. No caso de aparecerem linhas escuras, é uma indicação de substituição da foto ou dos dados. Padrões discordantes revelam a substituição de foto. Números e letras visíveis indicam alterações nos dados bibliográficos. Uma área não reflexiva indica que uma falsificação tenha sido cometida.

DOVID: Diffractive Optically Variable Image Device

Incluem hologramas e cinegramas. São produzidos através da gravação de micro perfis em filmes termoplásticos. Enquanto os hologramas são criados através da interferência de raios luminosos, os cinegramas são produzidos através de um método único não-holográfico. Os micro perfis de um cinegrama são projetados para produzir um brilho máximo de fácil verificação e de difícil falsificação. Ainda, efeitos ópticos podem ser aplicados aos cinegramas. O período dos micro perfis são tipicamente da ordem do comprimento de onda da luz incidente causando a difração da luz.

- Holografia: é um processo de registro de imagens, através de um fenômeno de interferência luminosa, que permite a reconstrução e visualização dessas imagens em três dimensões. O holograma é uma grade de difração complexa originária de um processo holográfico conforme podemos observar na Figura 4-9.

Figura 4-9 – Holografia
Fonte: www.spring.net

- Cinegrama: Os cinegramas são produzidos em folhas metalizadas no formato de um crescente. A imagem é formada por linhas finíssimas de diferente espessura e formato. Conforme se muda o ângulo da luz incidente, a imagem do cinegrama também muda, produzindo o efeito de movimento. Como podemos observar na Figura 4-10, ao movê-la sobre seu eixo vertical da esquerda para a direita, aparece uma pequena letra “k” no canto direito inferior. O tamanho da letra aumenta gradualmente em direção ao centro do cinegrama, onde encontra uma letra “S” maiúscula, ilustrando a sigla da unidade monetária da República Tcheca. Movendo-se um pouco mais o cinegrama, a letra “S” se torna um crescente, aumentando devagar até formar uma lua cheia contra o fundo escuro. Quando o cinegrama é movido sobre seu eixo horizontal, os dígitos “5000” aparecem à esquerda, correndo para cima mudando de claro para escuro e vice-versa. No fundo de um cinegrama, existem seis círculos aumentando proporcionalmente com textos e microtextos repetidos.

Figura 4-10 – Cinegrama
Fonte: www.nbs.sk

Quando um cinegrama é iluminado com luz branca, a imagem pode aparecer em furta cor. Uma característica importante da segurança do cinegrama é a habilidade de passar a idéia de movimento através da imagem, como se movesse de um lado para outro ou circularmente, permitindo uma fácil inspeção.

- Microestruturas de primeira ordem
    - Genéricas (Holográficas): 2-D, multi-plano (2-D/3-D), arco-íris (3-D), Estereograma: Moviegram™, Maxigram™.
    - Geradas por computador: Feixe de laser ou matriz de pontos: Trustseal™, Gyrogram™, OVM™, Feixe de laser ou elétrons: Kinegram®, Exelgram™.
    - Multigramas: combinações das técnicas acima
- Microestruturas de ordem zero (ZOD)

Dispositivos "Non-Iridescent"

- Perfuração a laser.h
- Imagens cauterizadas.
- Imagens inclinadas a laser (Figura 4-11): usando superfície lenticular e cauterização com laser.
- Imagens latentes.

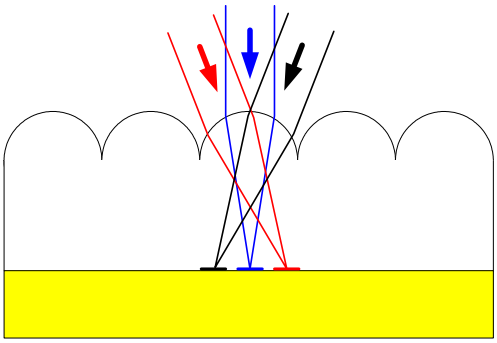


Figura 4-11 – Exemplo de dispositivo com estrutura “Non-Iridescent” (TLI lenticular)
Fonte: adaptado de www.laseroptical.co.uk

4.2.2. Nível 2: Inspeção com equipamentos simples

4.2.2.1. Micro Impressão

Consiste na impressão de micro textos ou imagens com tecnologia de offset. A largura mínima de linha em equipamento offset é de aproximadamente 10 micrometros, cerca de 4 vezes mais fina que uma linha de uma impressora com resolução de 600 DPI, conforme ilustrado na Tabela 4-1.

Tabela 4-1 – Micro impressão: limitações de impressão

Técnica de impressão	Largura de linha mínima [i]
Offset	~10 microns
Copiadora 600 DPI	~ 40 microns
Copiadora 400 DPI	~ 60 microns

[i] 25 microns = 1/1000 polegadas

- Micro Impressão (texto): Consistem na impressão de textos com linhas de espessura inferior a 20 micrometros, que são visíveis somente com uso de lentes de aumento. Aparecem como finas linhas contínuas de fundo do cartão e quando são reproduzidas por copiadoras ou digitalizadas e reimpressas, não são passíveis de reprodução, aparecendo permanentemente como linhas continuas, conforme exemplificado na Figura 4-12.

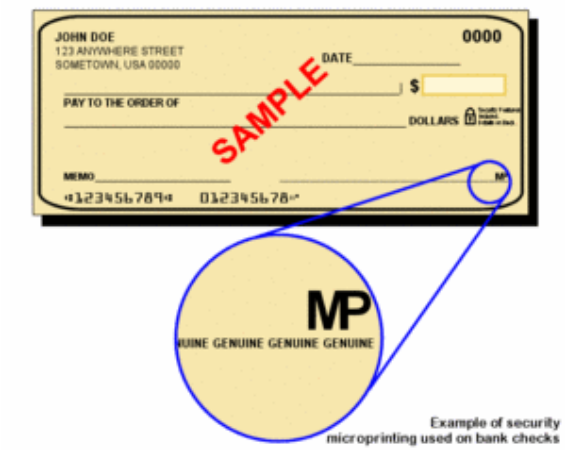


Figura 4-12 – Micro impressão (texto)
Fonte: www.answers.com

- Micro impressão (imagens): imagens impressas com resolução inferior a 20 microns que não aparecem quando são reproduzidas por copiadoras ou digitalizadas e reimpressas.

- Variações na espessura da linha.

4.2.2.2. Impressão com tintas especiais de segurança invisíveis a olho nú

- Impressão Ultra Violeta (UV): Tintas ultra violetas, invisíveis a olho nu, podem ser identificadas com uso de uma fonte de luz ultra violeta. Pode-se utilizar tintas UV tanto para altas quanto de baixas freqüências (Figura 4-13).

Figura 4-13 – Tinta fluorescente sensibilizada por UV
Fonte: www.entas.hu

- Impressão Infravermelho (IR): Tintas fluorescentes e tintas absorventes com a presença de luz infravermelha.

- Tintas “Metameric”: Trabalham com o princípio onde 2 cores combinadas sob um conjunto de luzes específicas podem aparecer diferentes sob um outro conjunto de

luzes. O efeito pode ser observado na Figura 4-14. Sob condições normais, nada é visível, porém o número “20” aparece quando observado sob um filtro vermelho.

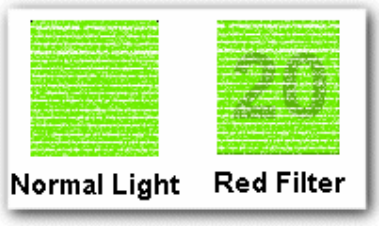


Figura 4-14 – Tinta “metameric”
Fonte: www.indigoimage.com

4.2.2.3. Tecnologias utilizando Leitoras

O desenho do cartão pode incluir varias tecnologias para recuperação de dados através de leitoras tais como tarja magnética, código de barras, chips (smart card) e hologramas. Verificação da autenticidade do documento, dos dados e /ou da pessoa que esta apresentando o documento pode ser verificada por um leitor. Técnicas comuns são dígitos verificadores, criptografia de dados e assinatura digital.

4.2.2.4. Tecnologias usando imagens geradas por computador

- DataGlyph :

Tecnologia para codificar dados em papel ou qualquer outro meio físico. A informação é codificada em milhares de pequenos elementos chamados “Grifos”. Cada elemento consiste de uma pequena linha diagonal a 45 graus de inclinação, do tamanho de 1 centésimo de polegada ou menos dependendo da resolução da impressão. Cada elemento representa um único binário 0 ou 1, dependendo se a inclinação é à esquerda ou à direita, como mostrado na Figura 4-15. Estes elementos em seqüência são usados para codificar informações numéricas e textuais.

Figura 4-15 – Dataglyph™
Fonte: www.xerox.com

Os elementos são agrupados formando imagens sem obstruir a leitura mesmo de textos, inclusive o padrão diagonal foi escolhido por causar menor distração visual. É possível armazenar milhares de caracteres escondidos em um padrão acinzentado de meio tom na forma de padrões de fundo ou qualquer elemento gráfico, sem serem percebidos.

A impressão destes elementos não acarreta diferenças no processo normal de impressão. A informação a ser gravada é codificada numa seqüência de "Grifos" formando pequenas áreas que contem uma espécie de esqueleto de sincronização embutida, repetindo um padrão fixo de elementos marcando as fronteiras dessas áreas e também servindo de clock para a leitura.

Antes dos dados serem colocados nas janelas de sincronização, eles são agrupados em blocos de alguns bytes e então se adicionam códigos de correção. A quantidade de códigos de correção a ser usado depende da aplicação desejada. Altos níveis de correção aumentam a área do desenho.

Por fim, os blocos de dados são dispersos aleatoriamente pela área do desenho, pois caso alguma parte do desenho seja danificada, torna-se possível de se recuperar a informação pela correção de erros.

- Digimarc

É uma marca d'água digital embutida em uma imagem de forma quase imperceptível em qualquer conteúdo digital. Um software insere informações imperceptíves fazendo modificações sutis nos dados da imagem original. Essas marcas d'água podem ser lidas para a validação de conteúdos originais ou autenticação de documentos, como mostra a Figura 4-16

A alteração provocada na imagem é muito sutil. Conforme a Figura 4-16 , é possível comparar a imagem original e a imagem codificada.

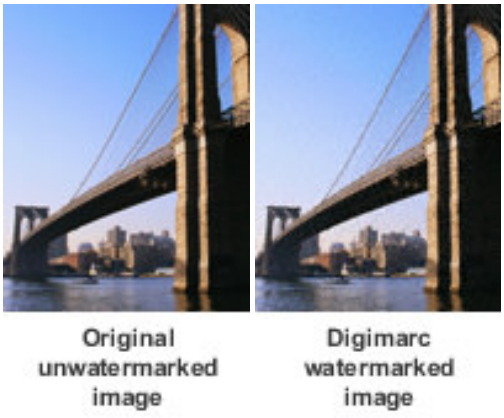


Figura 4-16 – Digimark
Fonte: www.insidegraphics.com

- Scrambled Indicia

É um processo de pré-impressão que mistura, embaralha e manipula imagens inserindo informação codificada ilegíveis a olho nu e protegidas contra cópias. Depois de impressas as imagens são decodificadas através de lentes que permitem ver imagens codificadas, como mostrado na Figura 4-17.

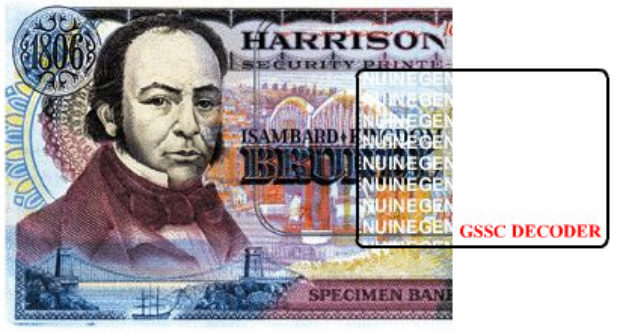


Figura 4-17 - Scrambled Indicia™
Fonte: www.graphicsecurity.com

- Copy Ban + Pantografia

Juntamente com a impressão prismática, essa técnica provê proteção contra duplicação a partir de scanners e impressoras digitais de desktop.

Figura 4-18 – Copy Ban™
Fonte: www.graphicsecurity.com

SafeCopyVoid™

Utiliza imagens embutidas que uma vez copiadas mostram avisos do tipo: ilegal ou nulo, como monstrado na Figura 4-19.

Figura 4-19 – SafeCopyVoid™
Fonte: www.graphicsecurity.com

4.2.3. Nível 3: Inspeção com dispositivos especiais

4.2.3.1. Tintas especiais

Tintas especiais desenvolvidas com elementos específicos que reagem a uma fonte de energia eletromagnética emitida por um leitor remoto. O uso desses tintas e medindo sua reflexão, é possível identificar um grupo determinado de cartões.. Estas tintas são chamadas de tintas inteligentes.

4.2.3.2. Materiais ocultamente embutidos

Ligando padrões pseudo-aleatórios com a informação do cartão.

- Óptico (assinaturas de luz): Copytex, fibras de polímeros
- Magnético: NHK, MagnaPrint
- RF: Bakeart, Inkode

- Marcas moleculares: Isotag
- Microtaggants

4.2.3.3. Texto seguro

Tecnologias de imagem de alta resolução tornam possivel a incorporação de microtextos, arte em linhas e criptografia de pixels como mostra a Figura 4-20.

Figura 4-20 – Texto Seguro
Fonte: www.hologrammachine.com

4.2.3.4. Imagem oculta sensível ao Laser

Esta tecnologia camaflada permite ao examinador ler uma mensagem de texto utilizando a incidência de Laser comum para autenticar uma imagem opticamente variável conforme a Figura 4-21.

Figura 4-21 – Imagem escondida recuperada a laser
Fonte: www.hologrammachine.com

4.2.4. Efetividades de técnicas para proteção de documentos

A Figura 4-22 ilustra a efetividade de técnicas de proteção de documentos em papel.

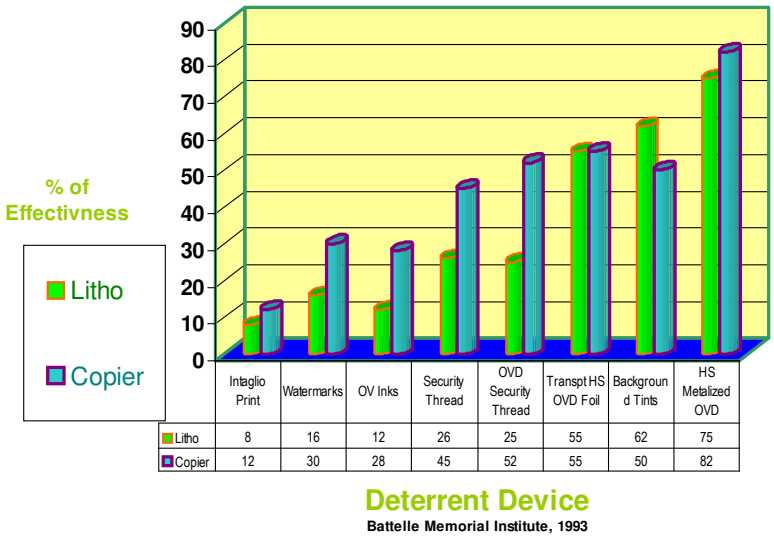


Figura 4-22 – Efetividade de técnicas de proteção

4.3. ITENS DE SEGURANÇA DE IMPRESSÃO DE DADOS VARIÁVEIS (PERSONALIZAÇÃO)

Os dados variáveis ou dados de personalização são os dados inseridos na customização individual de cada cartão com as informações do portador e requerem tanto segurança física quanto lógica.

A segurança física leva em consideração desde o processo envolvido na inserção dos dados até os mecansmos de segurança na tecnologia de impressão, procurando assim, reduzir os riscos de fraude e aumentar a segurança na autenticação do portador.

A segurança lógica tem por objetivo garantir segurança nas transações off-line e prover a privacidade em relação aos dados do portador, protegendo o acesso, leitura e escrita no caso dos smart cards.

Seguem algumas tecnologias de segurança na impressão dos dados variáveis.

4.3.1. Dados redundantes

Os dados são mostrados em mais de uma localização no documento, aumentando a resistência à alteração. Uma inspeção visual simples é requerida para determinar se todos os campos conferem. Dados redundantes podem também ser impressos em cores e fontes diferentes.

4.3.2. Dados Sobrepostos

Dados variáveis tais como uma assinatura digitalizada ou texto, podem ser inscrito sobre outro campo de dados, tais como foto. Esta técnica torna necessário alterar ambos os campos se um deles for alterado conforme a Figura 4-23.

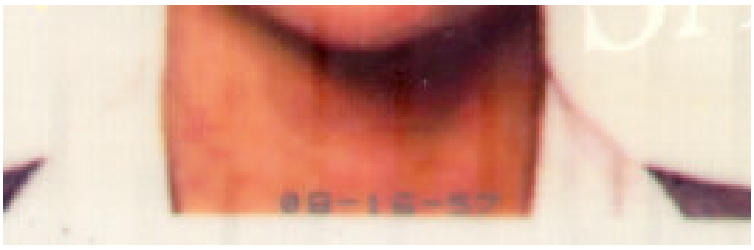


Figura 4-23 – Dados sobrepostos
Fonte: www.extension.ucsd.edu

4.3.3. Imagem Fantasma

visíveis e invisíveis (UV): Utiliza impressão de uma segunda imagem de um campo de dados do cartão, utilizando reprodução em meio tom da imagem original que é normalmente impresso na mesma área do dado original. Qualquer tentativa de alteração da imagem principal irá requerer a alteração da sua imagem fantasma.

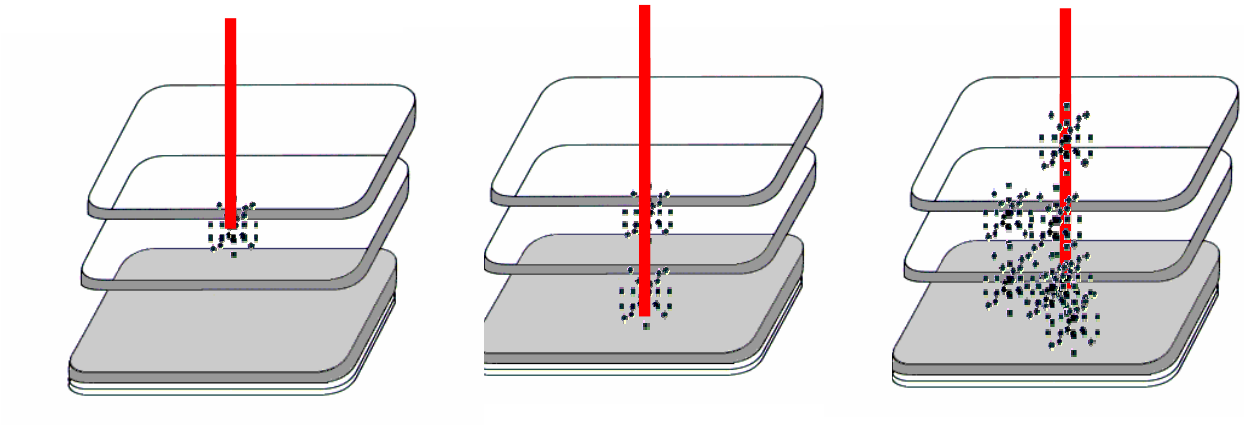
Figura 4-24 – Imagem Fantasma
Fonte: Datacard – Comunicações privadas

4.3.4. Erros deliberados

O uso de pequenos erros deliberados tais como a inversão de letras ou a falta ou duplicação de uma letra podem ser utilizados para checagem da autenticidade do documento. Estes erros não são revelados ao público em geral e são utilizados para pelas autoridades para checar a autenticidade de documentos falsificados e que tem os erros corrigidos pelos contraventores.

4.3.5. Impressão de dados variáveis e foto com *laser engrave*:

Tecnologia mais indicada para impressão de dados variáveis em cartões consiste em gravar as informações no cartão utilizando um feixe de laser para atingir a camada interna (núcleo) do cartão produzindo ali uma imagem através da queima do material (Figura 4-25). Garante que a impressão feita irá durar enquanto o cartão durar, pois caso contrário o mesmo para ser alterado será destruído no processo. O laser engrave permite ainda duas formas de impressão, uma delas vetorial e chamada "pixel". Isso permite que a gravação feita vetorialmente tenha sentido táctil no documento adicionando mais esta característica de segurança ao documento.



- ✓ O feixe "Laser" atravessa o cristal do cartão
- ✓ Não há reação
- ✓ O feixe "Laser" atinge a camada "laser"
- ✓ O pigmento desta camada reage imediatamente.

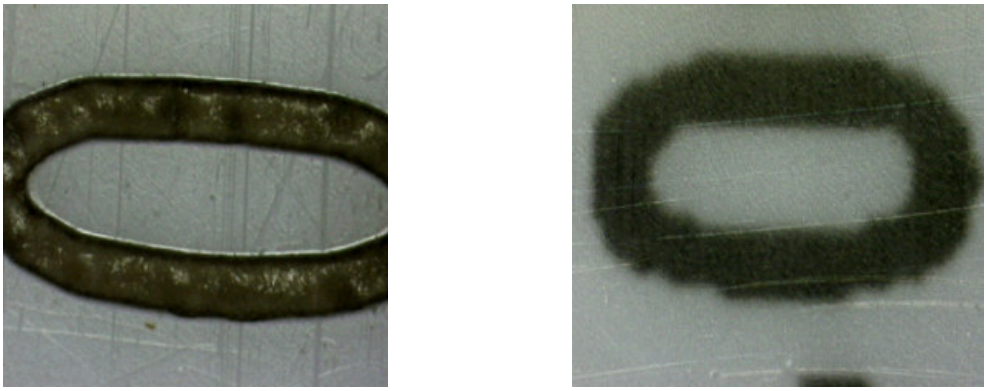
- ✓ O feixe "Laser" então atinge a núcleo do cartão
- ✓ O material reage imediatamente
- ✓ A interação entre os diferentes materiais então começa.

- ✓ Maior energia é enviada através do feixe "Laser"
- ✓ Os materiais continuam reagindo e aumentando sua temperatura.
- ✓ Então os pigmentos existentes na camada "laser" impregnam o cristal no seu lado interno finalizando a impressão.

Figura 4-25 – Laser engrave

Esta Tecnologia garante que a impressão feita irá durar enquanto o cartão durar, pois o mesmo, para ser alterado, será destruído no processo.

O Lazer Engrave permite ainda duas formas de impressão, uma vetorial e outra chamada “Pixel”. Isso permite que a gravação feita vetorialmente tenha sentido Táctil no documento adicionando mais esta característica de segurança ao documento (Figura 4-26).



Vetorial Pixel

Figura 4-26 – Tipos de laser engrave
Fonte: Datacard – Comunicações privadas

Figura 4-27 - Exemplo de documento Laser Engrave
Fonte: www.paspoortinformatie.nl

4.3.6. Impressão por transferência de matéria - *Grafix*

É um processo de impressão onde a tinta é transferrida para o cartão através de temperatura e pressão, ficando apenas na superfície do cartão. A tinta consiste na combinação

de pigmentos e resina, podendo se apresentar em uma variadade de cores, onde as cores escuras mostram-se mais duráveis do que cores claras.

Segue a ordem das mais duráveis para as menos duráveis:

- Preto, prata, vermelho, azul, verde, branco e dourado;

Para se ter uma idéia, as impressões em preto duram duas vezes mais que impressões em branco.

4.3.7. Combinação *Laser engrave* e por transferência de matéria (*Grafix*)

As duas técnicas anteriores podem ser combinadas para multiplicar a segurança conforme a Figura 4-28.

Figura 4-28 – Combinação de impressão de fotografia colorida e com laser engrave
Fonte: www.extension.ucsd.edu

4.3.8. Impressão de texto com fontes pequenas:

Difícil de detectar a olho nu, restringe o uso de scanners e não pode ser reproduzida por copiadora digital (Figura 4-29).

Figura 4-29 – Impressão com fontes pequenas
Fonte: www.extension.ucsd.edu

4.3.9. Camada/capa de proteção:

Cobertura com lâmina de material transparente, possivelmente contendo outros dispositivos de segurança. Esta camada visa proteger o cartão da exposição a químicos, abrasão e humidade. Seguem alguns exemplos de lâminas de proteção.

4.3.9.1. Lâmina holográfica

Impossível de ser escaneada, extremamente difícil de ser falsificada/imitada, possui características claras e distintivas (Figura 4-30, Figura 4-31).

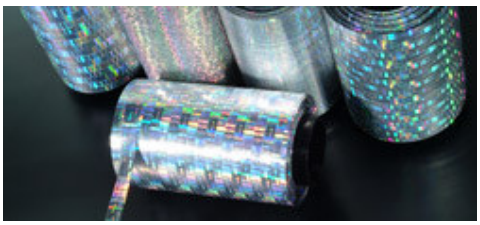


Figura 4-30 – Lâmina Holográfica

Figura 4-31 – Dispositivos de segurança OVD para cartões plásticos
Fonte: www.payne-security.com

4.3.9.2. Lâmina perolada

Conforme mostrado na Figura 4-32.

Figura 4-32 – Lâmina perolada
Fonte: Datacard– Comunicações privadas

4.3.9.3. Lâmina com impressão em UV

Conforme mostrado na Figura 4-33.

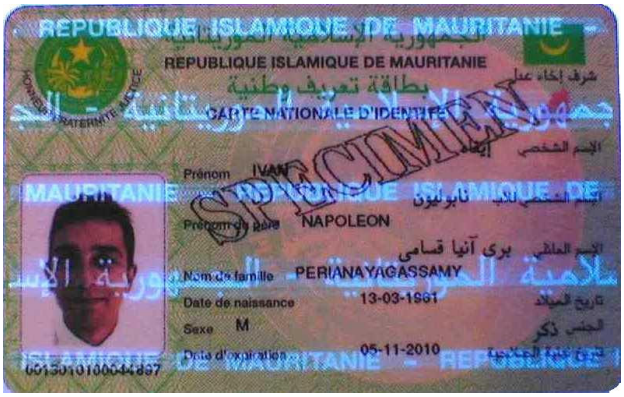


Figura 4-33 – Lâmina com impressão UV
Fonte: Datacard – Comunicações privadas

4.4. SEGURANÇA ELETRÔNICA IMPLEMENTADA NO CHIP (CRIPTOGRAFIA)

A segurança dos dados armazenados e acessados a partir do cartão deve ser garantida através de criptografia das informações, com base em algoritmos padronizados ou proprietários (pode ser desejável o uso de algoritmos de criptografia que não sejam públicos [49]), uso de chaves criptográficas adequadas e cuidados tecnológicos e de processos com o armazenamento e acesso dos dados e chaves dos usuários.

Considerando-se a aplicação como identidade eletrônica/título eleitoral, recomenda-se o uso do cartão inteligente como mídia que garante alto nível de proteção e portabilidade.

Para assegurar a autenticidade e a confidencialidade das informações trocadas nas comunicações com o cartão (sistemas<->cartão), algoritmos de criptografia devem ser utilizados, sendo que algoritmos de criptografia assimétrica apresentam maior nível de segurança aliados à geração de chaves pública e privada no hardware, as quais devem ter no mínimo 1024 bits de tamanho.

Algoritmos criptográficos suportados pelo chip

- Criptografia simétrica.
- Criptografia assimétrica.
- Funções de hash.
- Assinatura digital.

4.4.1. Autenticação e confidencialidade dos dados armazenados no cartão

4.4.1.1. Assinatura digital dos dados armazenados no cartão

- Assinatura digital dos dados armazenados no cartão, usando SHA1 e RSA, através de protocoladora digital [49].

4.4.1.2. Criptografia de dados transferidos do cartão para a aplicação

- Criptografia (simétrica) dos dados na comunicação.

4.4.2. Certificado Digital Pessoal

O ICP Brasil (Infra-estrutura de Chaves Públicas) possui classificações de certificados estabelecendo a rigorosidade de níveis de segurança.

Certificados de tipos A1, A2, A3 e A4 são utilizados em aplicações como confirmação de identidade na *Web*, correio eletrônico, transações *on-line*, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

Certificados de tipos S1, S2, S3 e S4 são utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

A Tabela 4-2 apresenta os requisitos mínimos para obter os certificados. Há incremento do nível de segurança crescente entre os certificados de tipos 1 a 4.

Tabela 4-2 - Requisitos ICP Brasil

Tipo de Certificado	Chave Criptográfica			Validade (anos)
	Tamanho da chave (bits)	Mecanismo de Geração da Chave	Mídia de Armazenamento	
A1 e S1	1024	SW	Cartão inteligente ou token, ambos sem capacidade de geração de chave e protegidos por senha	1
A2 e S2	1024	HW	Cartão inteligente ou token, ambos sem capacidade de geração de chave e protegidos por senha	2
A3 e S3	1024	HW	Cartão inteligente ou token, ambos com capacidade de geração de chave e protegidos por senha, ou hardware criptográfico pelo CG da ICP Brasil	3
A4 e S4	2048	HW	Cartão inteligente ou token, ambos com capacidade de geração de chave e protegidos por senha, ou hardware criptográfico aprovado pelo CG da ICP Brasil	3

4.4.2.1. Chaves para Certificado Digital

Mecanismo de Geração

Conforme já foi comentado em várias partes do documento, toda a segurança do processo baseia-se na garantia do sigilo da chave privada. Além da segurança do meio de armazenamento, o processo de geração e gravação da chave é um ponto de possibilidade de quebra da segurança. A geração das chaves criptográficas pode ocorrer de duas formas: por software e posterior armazenamento ou gerada diretamente pelo dispositivo de armazenamento.

Na geração externa ao dispositivo (software), as chaves são criadas por alguma entidade certificadora utilizando um dos tipos de algoritmos descritos anteriormente, sejam chaves públicas ou privadas. Desta forma, a chave privada, que deve ficar sob posse única e exclusivamente do usuário, é de alguma forma enviada para o dispositivo de armazenamento do usuário. Mesmo que o envio seja efetuado de maneira sigilosa, há um maior risco de vazamento de informações durante a criação, armazenamento e envio da chave ao usuário.

Por outro lado, caso a geração das chaves seja feita internamente no dispositivo de armazenamento (smart cards ou tokens), a chave privada não é transportada, aumentando-se o grau de segurança do processo como um todo. Esta forma de criação das chaves proporciona mais garantias de confidencialidade e autenticidade.

Assim, recomenda-se que as chaves pública e privada deverão ser geradas diretamente no smart card.

Comprimento

As chaves geradas possuem tamanhos determinados por bits. Naturalmente, quanto maior o número de bits, mais difícil é violação das chaves.

Atualmente chaves de 1024 bits possuem o tamanho mínimo para garantir a segurança. Porém é preciso considerar a evolução da tecnologia que facilita o trabalho de executar algoritmos cada vez mais rápido, permitindo que terceiros possam utilizar recursos computacionais para violar as chaves. Assim sendo, os 1024 a 2048 bits utilizados hoje, no futuro podem se tornar insuficientes para os níveis de segurança exigidos.

As chaves deverão ser geradas com 1024 bits, em conformidade com as chaves utilizadas em certificados ICP-Brasil A3/S3.

Armazenamento

Apesar da segurança lógica da chave privada, que conta com acesso restrito através de senha, os níveis de proteção variam também de acordo com a mídia utilizada para seu armazenamento. Na Tabela 4-3 são apresentadas as características dos níveis de proteção atingidos segundo a mídia utilizada, além de propriedades de portabilidade e custo.

Tabela 4-3 - Comparação entre tipos de mídias de armazenamento

Mídia	Nível de Proteção	Portabilidade	Custo*
HD	+	Não portável	Sem custo
CD	+ +	Portável	Baixo custo
Cartão Inteligente	+ + + +	Portável	Alto custo **
Token	+ + +	Portável	Médio custo

*considerando-se que o usuário já possua um computador

**considerando-se o conjunto leitora + cartão inteligente

As chaves deverão ser armazenadas no próprio smart card.

Acesso à chave privada

- O acesso à chave privada deverá ocorrer apenas mediante apresentação de PIN (senha).

Operações criptográficas com a chave privada

- Deverão ser realizadas exclusivamente no smart card.

4.4.3. PCC (Proof-carrying code)

- Código móvel (e.g. applet) que contém uma prova criptográfica de que o código está conforme com uma política de segurança dada (autenticação de código).

- Para cartões multi-aplicação.

5. PROPOSTA DE UM NOVO DOCUMENTO DE IDENTIFICAÇÃO ELETRÔNICA (E-ID) PARA O BRASIL

Neste capítulo é apresentada uma proposta para um novo documento de identificação eletrônica para o Brasil. Essa proposta tem por premissa a adoção de um documento em cartão plástico do tipo cartão inteligente (smart card). Desse modo o cartão poderá ser lido eletronicamente e seja usado como parte do processo de verificação e autenticação da identidade do cidadão, portador do novo documento.

O estabelecimento de premissas básicas acerca da utilização do documento de identificação é realizado a partir de um conceito de modelos de verificação e autenticação da identidade. Consideram-se, para efeito de autenticação da identidade três componentes: o que se tem,o que se é e o que se sabe.

O que se tem é o próprio documento de identificação, que deve estar em posse do cidadão durante o processo de verificação e autenticação da identidade sempre que esse componente for requerido neste processo.

O que se é está essencialmente relacionado às informações biográficas (nome, data de nascimento, naturalidade etc.) e bimométricas disponíveis aos processos de identificação e de verificação e autenticação da identidade. No que diz respeito às informações biográficas e biométricas, define-se os campos a serem impressos e armazenados eletronicamente no cartão em função da legislação em vigor atualmente. No que diz respeito às informações biométricas especificamente, é desejável que o novo documento possa introduzir um processo automatizado de verificação da identidade, auxiliado por técnicas biométricas. Não é escopo deste trabalho fazer uma análise dos mecanismos automatizados de identificação biométricas disponíveis na atualialidade (íris, impressões digitais, fotografia de face etc.), nem tampouco dos processos para coletar as informções biométricas necessãrias, quando elas ainda não estiverem disponíveis, com o formato e a qualidade requeridos, nos arquivos dos órgãos públicos responsáveis pela identificação e emissão dos documentos de identificação. Discussões acerca deste tema podem ser encontradas em [48].

Neste trabalho considera-se que a identificação biométrica automatizada deve ser feita através de um sistema de identificação biométrica automatizado usando impressões digitais (AFIS). Tal sistema consiste essencilmente de uma base de dados contendo a informação

biométrica (i.e. impressões digitais) dos indivíduoes identificados (i.e. indivíduos que tiveram seu documento de identidade emitido). Com uso de técnicas biométricas apropriadas [2] é possível identificar um indivíduo que esteja cadastrado nesta base de dados a partir da coleta de uma de suas impressões digitais. Esse processo de identificação envolve uma busca comparativa da nova impressão digital coletada com as demais registradas no bando de dados, dita comparação 1:N (um para N), onde N denota o número de indivíduos registrados na base de dados. Esse processo, ainda que possa ser essencial para algumas aplicações específicas (e.g. investigações criminais), é complexo e caro devido à necessidade de se ter acesso à base de dados biométricos completa e a infra-estrutura computacional para se fazer a busca contra potencilamente milhões de registros. Entretanto, se a(s) impressão(ões) digital(is) do indivíduo puderem estar disponíveis durante o processo de verificação e autenticação da identidade, é possível fazer uma comparação única, dita comparação 1:1 (um para um), entre a nova impressão digital coletada e a impressão digital correspondente coletada durante o cadastramento na base de dados. Desse modo, considera-se que as impressões digitais coletadas no cadastramento deve ser seguramente armazenadas eletronicamente no cartão, permitindo que elas possam ser lidas e usadas no processo de verificação e autenticação da identidade. Assim, é possível obter-se altos níveis de confiabilidade no processo automatizado de verificação da identidade a partir de uma combinação entre o que se tem (cartão) e o que se é (impressão digital).

O que se sabe é geralmente uma senha pessoal (PIN) ou uma chave criptográfica que permita, por exemplo, realizar assinaturas digitais verificáveis. Neste caso específico destaca-se o uso de certificação digital em uma infra-estrutura de chaves públicas (ICP) como forma prover um serviço não apenas de autenticação da identidade, mas de assinaturas digitais irrepudiáveis [30]. Para que isso seja possível, o chip do cartão inteligente deve ser capaz de armazenar certificados digitais e realizar funções criptográficas apropriadas.

Um outro aspecto importante e que tem implicações na concepção e definição do novo documento é se o cartão terá finalidade única ou se ele se tornará um documento multiaplicativo. Essa discussão se coloca num contexto sócio, político, cultural e econômico onde diversas aplicações de natureza pública e privada (e.g. programas sociais, pagamento de benefícios, sistema eleitoral, controle de condutores de veículos automores, sistema bancário, controle de passageiros aéreos) podem se beneficiar de um mecanismos confiável de verificação da identidade.

Essa utilização determina igulamente o valor dos documentos, em termos das informações neles armazenadas e das aplicações que passam a utilizar o mecanismo de verificação e autenticação da identidade suportado pelo modelo de documento definido. Isso é importante, uma vez que os requistos funcionais associados às funções de processamento e memória disponíveis do chip, o tipo de material plástico utilizado, assim como os requisitos de segurança implementados sejam compatibilizados com o valor e o uso que o novo documento deverá ter.

Como não há uma solução única para todos os cenários possíveis de utilização de um cartão de identificação com abrangência nacional, propõe-se alternativas para as recomendações técnicas que definem o novo documento considerando alguns cenários de utilização mais provavéis:

- Cenário 1: Cartão de aplicação simples, com verificação automática da identidade do portador apenas através de biometria.
- Cenário 2: Cartão de aplicação simples, com verificação automática da identidade do portador apenas através de biometria e suporte a certificação digital.
- Cenário 3: Cartão multi-aplicação, com verificação automática da identidade do portador apenas através de biometria.e suporte a certificação digital.

No que diz respeito ao material utilizado para confecção do cartão plástico, adota-se como premissa a definição de um cartão de longa vida, com durabilidade de até 10 anos.

Finalmente, no que diz respeito à segurança do documento, a proposta segue uma abordagem de custo benefício, indicando vários dispositivos de segurança que podem ser agregados e o custo relativo desses mecanismos.

5.1. DADOS IMPRESSOS E ARMAZENADOS NO CARTÃO

5.1.1. Análise da legislação

No contexto da concepção e desenvolvimento dessa proposta, considera-se a definição e normatização de um novo Cartão Nacional de Identificação, conforme disposto na Lei 9.454, de 07 de abril de 1997 :

O art. 1º estabelece a instituição do número único de Registro de Identidade Civil.

A criação do Cadastro Nacional de Registro de Identidade Civil, destinado a conter o número único de Registro Civil, acompanhado dos dados de identificação de cada cidadão, é estabelecida no art. 2º.

O art. 3º define a forma de controle da centralização das informações e a atuação das Unidades da Federação e dos Municípios na operacionalização das atividades.

A Lei 9.454 supracitada ainda não foi regulamentada, apesar de definir, em seu artigo 5°, prazos para regulamentação, início de implantação e, no artigo 6°, prazos para a perda de validade dos documentos de identidade antigos (e.g. RG)[7].

O conteúdo informacional impresso na carteira de identificação civil (RG) atual está especificado na Lei 7.116 de 29 de agosto de 1983, regulamentada pelo Decreto 89.250 (27/12/1983), alterado pelo Decreto 2.170 (04/03/1997), e ainda pelo disposto nas Leis 9.049 (faculta o registro de informações no documento de identificação civil) e 9.434 (Lei de Remoção de Órgão e Tecidos para Transplante).

5.1.2. Campos impressos no cartão e armazenados no chip

Com base nesta legislação, propõem-se, na Tabela 5-1 a seguir, os campos propostos para o novo modelo do Cartão Nacional de identificação, no que diz respeito à identificação do documento e aos dados biográficos de identificação/qualificação dos cidadãos.

Tabela 5-1 – Campos impressos e armazenados no cartão

Campo	Descrição	Obrigatório/ Opcional	Impresso	Armazenado
Emissor	Nome e logo do emissor (e.g. Armas da República e inscrição que identifique o	Obrigatório	Sim	Não

[7] Os documento de identificação civil (e.g. RG) não perderam a validade devido à edição sucessiva de medidas provisórias prorrogando a vigência desses títulos.

Tabela 5-1 – Campos impressos e armazenados no cartão				
Campo	Descrição	Obrigatório/ Opcional	Impresso	Armazenado
	emissor)			
Título de documento	Título do documento (e.g. Identidade civil)	Obrigatório	Sim	Não
Sobrenome	Último sobrenome	Obrigatório	Sim	Sim
Nome(s)	Nome(s) atribuídos e demais sobrenomes	Obrigatório	Sim	Sim
Filiação	Nomes do pai e da mãe	Obrigatório	Sim	Sim
Local de nascimento	Município de nascimento e unidade da federação e	Obrigatório	Sim	Sim
Data de nascimento	Formato : “DD-MM-CCYY”	Obrigatório	Sim	Sim
Número da inscrição	Número único de Registro Civil	Obrigatório	Sim	Sim
Assinatura do emissor	Assinatura do dirigente do órgão emissor	Obrigatório	Sim	Não
Dados do documento original	comarca, cartório, livro, folha e número do seu registro de nascimento ou casamento;	Opcional	Não	Não
CPF	Cadastro de pessoas físicas	Opcional	Sim	Sim
RG	identificação do órgão expedidor, registro geral no órgão emitente, local e data da expedição	Opcional	Não	Sim
Expressão	expressão "Idoso ou maior de sessenta e cinco anos";	Opcional	Sim	Sim
Expressão	"Doador de órgãos e tecidos" ou "Não-doador de órgãos e tecidos".	Opcional	Sim	Sim
Tipo sangüíneo	Tipo sangüíneo	Opcional	Sim	Sim
Tipo de documento	Código (internacional) para o tipo de documento (ISO 7810)	Opcional [i]	Não	Sim
Número Internacional do Documento	O número do documento é formado de acordo com a ISO 7812-1 e possui 19 dígitos contendo o código do país, código do emissor, e um número serial único. Este número poderá ser impresso em formatos especiais para maior segurança.	Opcional [ii]	Sim	Sim
Nacionalidade	Código de três dígitos [ISO 3166-1]. A ICAO acrescenta a esta lista códigos para refugiados e outros.	Opcional [ii]	Não	Sim

[i] Documento do tipo ID-1.
[ii] Apenas para aderência a normas internacionais de identificação.

Além dessas informações, o cartão conterá os seguintes dados biométricos do cidadão, mostrados na Tabela 5-2.

Tabela 5-2 – Campos impressos e armazenados no Cartão – Dados Biométricos				
Campo	Descrição	Obrigatório/ Opcional	Impresso	Armazenado
Fotografia	Fotografia, em tamanho mínimo de 26mm x 32mm	Obrigatório	Sim	Sim
Impressão digital	Template de 10 impressões digitais	Obrigatório	Não	Sim
Assinatura	Assinatura do portador [i]	Obrigatório [i]	Sim	Sim

[i] Este campo deve ser obrigatório para cidadãos alfabetizados que podem assinar seu próprio nome.

A Tabela 5-3 abaixo apresenta ainda alguns campos que devem ser integrados ao documento, com objetivo de conferir maior segurança e usabilidade ao documento.

Tabela 5-3 – Campos impressos e armazenados no Cartão – Dados Adicionais

Campo	Descrição	Obrigatório/ Opcional	Impresso	Armazenado
Assinaturas digitais	Assinaturas digitais para cada conjunto de registros.	Obrigatório	Não	Sim
Validade	Formato : "DD-MM-CCYY" [i]	Opcional [i]	Sim	Sim
Endereço	Logradouro, complemento, número, bairro, município e UF.	Opcional	Não	Sim
Certificado Digital	Certificado digital para o portador.	Opcional	Não	Sim

[i] O documento atual tem validade indeterminada. Dentre as vantagens de se colocar uma validade determinada ao documento destaca-se a necessidade de atualização de dados que mudam com a vida do eleitor, em especial, a fotografia.

5.1.3. Estrutura de dados e armazenamento no chip

A Tabela 5-4 apresenta a estrutura de registros a serem armazenados no chip do cartão com a estimativa do tamanho, em bytes, para cada registro.

Tabela 5-4 – Registro Armazenados no Cartão

Registro	Campos	Tamanho (bytes)
Título Eleitoral	Número de série do chip	3k
	Dados biográficos (nome, filiação, naturalidade, data de nascimento etc.)	
	Dados do Registro Eleitoral (número, zona etc.)	
	Número de documentos (CPF, RG)	
	Tipo de documento	
	Hash da foto + minúcias + assinatura	
	Validade	
Assinatura Digital do Título Eleitoral	Assinatura digital dos dados do título eleitoral	0,5k
Endereço[i]	Endereço do eleitor (opcional)	1k
Assinatura Digital do Endereço[i]	Assinatura digital do endereço (opcional)	0,5k
Foto	Foto de face	3k
Minúcias	Minúcias	10k
Assinatura do eleitor	Imagem da assinatura do eleitor	1k
Certificado digital pessoal	Certificado digital pessoal (opcional)	8k
Outras aplicações	Espaço reservado para outras aplicações (opcional)	5k
Total		32k

[i] Endereço e Assinatura Digital do Endereço são campos opcionais e aparecem como um registro separado para que se permita atualização sem reemissão do cartão. Caso esta não seja uma possibilidade viável, deve-se incluir o campo Endereço no registro Título Eleitoral e se excluir o registro de Assinatura Digital do Endereço.

5.2. CIRCUITO INTEGRADO (CHIP)

5.2.1. Dimensionamento de memória do chip

No processo de escolha do chip, um dos aspectos importantes é a memória disponível para armazenamento de dados. Para a escolha do tamanho nominal de memória do chip é importante considerar os seguintes aspectos:

- Tamanho necessário de armazenamento de dados. É calculado através do somatório do tamanho de todas os dados a serem armazenados no chip (certificados, identificadores, etc), conforme indicado na seção 5.1.3;
- Tamanho ocupado pelo sistema de arquivo geral do chip. Tudo que é armazenado no chip é mapeado no sistema de arquivo, ocupando assim um espaço um pouco maior que o tamanho lógico do dado;
- Parte da EEPROM é usada pelo sistema operacional do chip para execução de seus comandos, por exemplo, buffers temporários, pilhas de memórias etc.

Portanto, para a especificação do valor mínimo de memória necessária pelo cartão deve-se considerar o somatórios dos 3 fatores acima.

5.2.2. Recomendação e especificação

Para a definição do chip mais apropriado para determinada aplicação, é necessário conduzir uma análise considerando os seguintes critérios:

- Capacidade de Armazenamento de Dados.
- Segurança de Dados.
- Certificações e Padrões.
- Sistemas Operacionais do Chip.

Com base nos critérios citados acima, seguem as recomendações sobre as características mínimas que um chip deve possuir para atender as necessidades de uma cartão inteligente de identidade pessoal.

Foram considerados os três cenários definidos anteriormente para construão de especificações técnicas alternativas, resultando em chips diferentes para cada um dos casos. Entretanto, as especificações de um chip para o cenário 2 suportam totalmente as especificações definidas para o cenário 1. Do mesmo modo, as especificações para o cenário 3 suportam integralmente as especificações dos cenários 1 e 2, sugerindo a seguinte denominação:

- Cenário 1: Configuração obrigatória mínima.
- Cenário 2: Configuração desejável mínima.
- Cenário 3: Configuração desejável completa.

Vale resaltar que o custo relativo entre cada um desses chips cresce da configuração adotada proposta para o cenário 1 para a configuração proposta para o cenário 3.

5.2.3. Configuração obrigatória mínima

Neste cenário, o chip deverá ser capaz de armazenar as informações mínimas e requeridas para o projeto, armazenar assinaturas digitais para uma conferência externa e possuir a capacidade de realizar operações criptográficas simétricas.

Além disso, o chip deverá possuir um mecanismo para a proteção da memória EEPROM de ataques externos, possibilitar a configuração de senhas para o acesso a arquivos restritos bem como permitir a configuração das condições de acesso aos diferentes arquivos criados no chip.

5.2.3.1. Aderência a padrões

- Seguir, no mínimo, as regras estabelecidas para o nível 1 de segurança do padrão FIPS 140-1 ou 2;
- Seguir, no mínimo, as regras estabelecidas para o nível 2 de segurança do padrão FIPS 140-1 ou 2, para verificação de violação no hardware (Tamper Evidence);
- Ser compatível com as regras estabelecidas para no padrão Common Criteria versão 2.1 parte 2 ou superior;
- Aderir ao padrão ISO 7816 partes 1, 2, 3, 4, 5 e 6;
- Atender aos requisitos do padrão PC/SC versão 1.0 ou superior.

5.2.3.2. Características Gerais

- Possuir numeração única para cada dispositivo;
- Voltagem de operação de 3 a 5 V com +/- 10% de tolerância;
- Ser resistente à água;

5.2.3.3. Características Funcionais

- Permitir a configuração do número máximo de consecutivas de acerto do PIN (código de acesso do usuário) e do PUK (código de acesso do administrador);
- Permitir alteração/desbloqueio do PIN;
- Permitir a alteração do PUK;
- Permitir a criação de senha de acesso ao dispositivo de, no mínimo, 6 caracteres numéricos e alfanuméricos;
- Possuir mecanismo de *anti-tearing;*
- Permitir a personalização eletrônica através de parâmetro identificador interno (label);
- Suportar, no mínimo, 300.000 ciclos de escrita e leitura do chip.

5.2.3.4. Capacidade de armazenamento

- Possuir, no mínimo, 24 KB de memória EEPROM livre para aplicações;

5.2.3.5. Comunicação

- Ser compatível com leitoras que suportem os padrões: ISO 7816-3 e PC/SC e EVM96;
- Permitir comunicação com leitoras através do protocolo T=0;
- Possuir interface T=0 com velocidade mínima de 9.600 bps.
- Permitir comunicação com leitoras através do protocolo T=1;
- Possuir interface T=1 com velocidade mínima de 9.600 bps.

5.2.3.6. Itens de Segurança

- Suportar algoritmos de criptografia simétricos (DES ou 3DES – 2 ou 3 chaves);
- Utilizar o algoritmo simétrico 3-DES ou AES com chaves de no mínimo 128 bits, para cifrar as chaves privadas armazenadas;

- O algoritmo simétrico 3DES deve utilizar três chaves distintas (k1, k2 e k3), geradas por derivação, a partir de um código de acesso escolhido pelo titular do repositório;
- O algoritmo simétrico AES deve ter sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório.
- Permitir a definição de política de segurança.
    - Forçar a troca da senha padrão no primeiro acesso;
    - A utilização do dispositivo deve ser bloqueada após 5 tentativas de autenticação com códigos inválidos;
- Possuir *firewall* para a proteção da memória;
- Calcular CRC de blocos aderindo aos padrões da ISO 3309.

5.2.3.7. Plataformas Suportadas

- Possuir driver disponíveis para o sistema operacional Linux kernel 2.4 e versões superiores estáveis;
- Possuir driver disponíveis para o sistema operacional Microsoft Windows 98 SE e versões superiores.

5.2.3.8. Gerenciamento do dispositivo

- Possuir um utilitário com interface gráfica em idioma português do Brasil, que permita gerenciamento do dispositivo;
- Permitir o apagamento de dados contidos no dispositivo, após autenticação do titular;
- Permitir a reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso.

5.2.4. Configuração desejável mínima

Neste cenário, o chip deverá ser capaz de armazenar as informações mínimas e requeridas para o projeto, assinar, criptografar e descriptografar dados através de criptografia assimétrica e possuir a capacidade de realizar operações de criptografia simétrica.

Além disso, o chip deverá possuir um mecanismo para a proteção da memória EEPROM de ataques externos, possibilitar a configuração de senhas para o acesso a arquivos restritos bem como permitir a configuração das condições de acesso aos diferentes arquivos

criados no chip e impedir que as chaves privadas armazenadas estejam disponíveis para o mundo externo.

5.2.4.1. Aderência a padrões

- Ser compatível com as regras estabelecidas para o nível 1 de segurança do padrão FIPS 140-2 e as regras estabelecidas no padrão Common Criteria versão 2.1 parte 2 ou superior;
- Ser compatível com as regras estabelecidas para o nível 2 de segurança do padrão FIPS 140-2, para verificação de violação no hardware (*Tamper Evidence*) e as regras estabelecidas no padrão Common Criteria 2.1 parte 3 e EAL 4+ ou superior.
- Aderir ao padrão ISO 7816 partes 1, 2, 3, 4, 5, 6, 8 e 9;
- Atender aos requisitos do padrão PC/SC versão 1.0 ou superior.

5.2.4.2. Características Gerais

- Voltagem de operação de 3 a 5 V com +/- 10% de tolerância;
- Possuir numeração única para cada dispositivo;
- Ser resistente à água;

5.2.4.3. Características Funcionais

- Permitir o armazenamento de certificados digitais e seus pares de chaves (tamanho 2048 bits RSA);
- Permitir a configuração do número máximo de consecutivas de acerto do PIN (código de acesso do usuário) e do PUK (código de acesso do administrador);
- Permitir alteração/desbloqueio do PIN;
- Permitir a alteração do PUK;
- Permitir a exportação de certificados armazenados no dispositivo para o *Certificate Store* ambiente Microsoft Windows 98 SE e versões superiores;
- Permitir a personalização eletrônica através de parâmetro identificador interno (label);
- Permitir a criação de senha de acesso ao dispositivo de, no mínimo, 6 caracteres numéricos e alfanuméricos;
- Suportar o gerenciamento de ciclo de vida;
- Possuir mecanismo de *anti-tearing;*

- Suportar, no mínimo, 300.000 ciclos de escrita e leitura do chip.

5.2.4.4. Capacidade de armazenamento

- Possuir, no mínimo, 32 kB de memória EEPROM livre para aplicações;
- Possuir, no mínimo, RAM = 2 kB.

5.2.4.5. Comunicação

- Ser compatível com leitoras que suportem os padrões: ISO 7816-3 e PC/SC;
- Permitir comunicação com leitoras através dos protocolos T=0 e T=1;
- Possuir interface T=0 com velocidade mínima de 9.600 bps;
- Possuir interface T=1 com velocidade mínima de 9.600 bps.

5.2.4.6. Interoperabilidade

- Possuir uma biblioteca de funções no padrão PKCS#11;
- Possuir um CSP (Cryptographic Service Provider) compatível com a CryptoAPI da Microsoft, para ambientes Microsoft® Windows 98 SE e versões superiores;
- Integração de certificados armazenados no dispositivo, com o NSS – Network Security Services, do ambiente Linux kernel 2.4 e versões superiores estáveis.

5.2.4.7. Itens de Segurança

- Atender aos requisitos da seção 4.7.2, do padrão FIPS 140-2, para a geração de chaves criptográficas;
- Gerar o par de chaves no hardware;
- Possuir capacidade de geração interna de chaves RSA sendo que as mídias destinadas ao armazenamento de certificados de nível de segurança 3 devem implementar a geração de chaves RSA com 512, 768, 1024 ou 2048 bits com ou sem CRT (Chinese Remainder Theorem);
- Suportar algoritmos de criptografia simétricos (DES, 3DES – 2 ou 3 chaves), algoritmos de criptografia assimétricos (RSA) e função de hash (SHA-1);
- Implementar o algoritmo RSA com SHA-1 como função hash, conforme o padrão PKCS#1 (RFC 2313).

- Permitir a gravação de chaves privadas e certificados digitais que utilizam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459;
- Implementar mecanismo de autenticação tipo *challenge-response*;
- Permitir a definição de política de segurança;
    - A ativação de funções que utilizem as chaves privadas só pode ser realizada após autenticação da identidade do titular do dispositivo;
    - Forçar a troca da senha padrão no primeiro acesso;
    - A utilização do dispositivo deve ser bloqueada após 5 tentativas de autenticação com códigos inválidos;
    - O titular do dispositivo deve ser avisado a cada vez que uma função que utilize sua chave privada tiver de ser ativada, e deve se autenticar para liberar a utilização pretendida;
- Possuir um *firewall* para a proteção da memória EEPROM;
- As rotinas de criptografia, que por característica do dispositivo, manipulem as chaves privadas em memória, devem:
    - Usar área de memória do tipo non-swappable;
    - Sobrescrever com valores fixos imediatamente após o término das funções que utilizaram estas chaves;
    - Rodar em kernel mode, como parte do núcleo do sistema operacional, no anel 0, também chamado de "supervisor mode".
- Não permitir que a chave privada, se gerada no dispositivo, seja exportada, condicionando as transações que utilizam a chave privada a ocorrer dentro deste.

5.2.4.8. Armazenamento de chaves privadas

- As chaves privadas devem ser armazenadas em repositório de dados próprio, controlado pela solução;
- Apenas certificados pertencentes a um único titular podem ser associados às chaves contidas num determinado dispositivo;
- Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 8kbytes;
- Utilizar o algoritmo simétrico 3-DES ou AES com chaves de no mínimo 128 bits, para cifrar as chaves privadas armazenadas;

- O algoritmo simétrico 3DES deve utilizar três chaves distintas (k1, k2 e k3), geradas por derivação, a partir de um código de acesso escolhido pelo titular do repositório;
- O algoritmo simétrico AES deve ter sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório.

5.2.4.9. Plataformas suportadas

- Possuir driver disponíveis para o sistema operacional Linux kernel 2.4 e versões superiores estáveis;
- Possuir driver disponíveis para o sistema operacional Microsoft Windows 98 SE e versões superiores;
- Suportar o browser Microsoft Internet Explorer a partir da versão 5.5;
- Suportar o browser Netscape Navigator a partir da versão 7.0 ou Mozilla a partir da versão 1.3.

5.2.4.10. Gerenciamento do dispositivo

- Possuir um utilitário com interface gráfica em idioma português do Brasil, que permita gerenciamento do dispositivo;
- Permitir a exportação de certificados armazenados no dispositivo;
- Permitir a importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo de acordo com a RFC 2315;
- Permitir a importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;
- Permitir a visualização de certificados armazenados no dispositivo;
- Permitir o apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular;
- Permitir a reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso.

5.2.4.11. Certificações

- Possuir certificação CC EAL 4+ ou superior.

5.2.5. Configuração Desejável Completa

Neste cenário, o chip deverá ser capaz de armazenar as informações mínimas e requeridas para o projeto, assinar, criptografar e descriptografar dados através de criptografia assimétrica e possuir a capacidade de realizar operações de criptografia simétrica.

Além disso, o chip deverá possuir um mecanismo para a proteção da memória EEPROM de ataques externos, possibilitar a configuração de senhas para o acesso a arquivos restritos bem como permitir a configuração das condições de acesso aos diferentes arquivos criados no chip e impedir que as chaves privadas armazenadas estejam disponíveis para o mundo externo.

Prevendo futuras alterações ao longo de seu uso, o chip deverá ser multi-aplicativo sendo capaz de carregar e excluir aplicações diversas.

5.2.5.1. Aderência a padrões

- Ser compatível com as regras estabelecidas para o nível 1 de segurança do padrão FIPS 140-2 e as regras estabelecidas no padrão Common Criteria versão 2.1 parte 2 ou superior;
- Ser compatível com as regras estabelecidas para o nível 2 de segurança do padrão FIPS 140-2, para verificação de violação no hardware (*Tamper Evidence*) e as regras estabelecidas no padrão Common Criteria 2.1 parte 3 e EAL 4+ ou superior.
- Aderir ao padrão ISO 7816 partes 1, 2, 3, 4, 5, 6, 8 e 9;
- Atender aos requisitos do padrão PC/SC versão 1.0 ou superior.
- Atender ao padrão Javacard.

5.2.5.2. Características Gerais

- Voltagem de operação de 3 a 5 V com +/- 10% de tolerância;
- Possuir numeração única para cada dispositivo;
- Ser resistente à água;
- Plataforma aberta;
- Multi-aplicativo.

5.2.5.3. Características Funcionais

- Permitir o armazenamento de certificados digitais e seus pares de chaves (tamanho 2048 bits RSA);
- Permitir a configuração do número máximo de consecutivas de acerto do PIN (código de acesso do usuário) e do PUK (código de acesso do administrador);
- Permitir instalar novas aplicações em qualquer ciclo de vida do cartão.
- Permitir alteração/desbloqueio do PIN;
- Permitir a alteração do PUK;
- Permitir a exportação de certificados armazenados no dispositivo para o *Certificate Store* ambiente Microsoft Windows 98 SE e versões superiores;
- Permitir a personalização eletrônica através de parâmetro identificador interno (label);
- Permitir a criação de senha de acesso ao dispositivo de, no mínimo, 6 caracteres numéricos e alfanuméricos;
- Suportar o gerenciamento de ciclo de vida;
- Possuir mecanismo de *anti-tearing;*
- Suportar, no mínimo, 300.000 ciclos de escrita e leitura do chip.

5.2.5.4. Capacidade de armazenamento

- Possuir, no mínimo, 32 KB de memória EEPROM livre para aplicações;
- Possuir, no mínimo, RAM = 2 KB.

5.2.5.5. Comunicação

- Ser compatível com leitoras que suportem os padrões: ISO 7816-3 e PC/SC;
- Permitir comunicação com leitoras através dos protocolos T=0 e T=1;
- Possuir interface T=0 com velocidade mínima de 9.600 bps;
- Possuir interface T=1 com velocidade mínima de 9.600 bps.

5.2.5.6. Interoperabilidade

- Possuir uma biblioteca de funções no padrão PKCS#11;
- Possuir um CSP (Cryptographic Service Provider) compatível com a CryptoAPI da Microsoft, para ambientes Microsoft® Windows 98 SE e versões superiores;

- Integração de certificados armazenados no dispositivo, com o NSS – Network Security Services, do ambiente Linux kernel 2.4 e versões superiores estáveis.

5.2.5.7. Itens de Segurança

- Atender aos requisitos da seção 4.7.2, do padrão FIPS 140-2, para a geração de chaves criptográficas;
- Gerar o par de chaves no hardware;
- Possuir capacidade de geração interna de chaves RSA sendo que as mídias destinadas ao armazenamento de certificados de nível de segurança 3 devem implementar a geração de chaves RSA com 512, 768, 1024 ou 2048 bits com ou sem CRT (Chinese Remainder Theorem);
- Suportar algoritmos de criptografia simétricos (DES, 3DES – 2 ou 3 chaves), algoritmos de criptografia assimétricos (RSA) e função de hash (SHA-1);
- Implementar o algoritmo RSA com SHA-1 como função hash, conforme o padrão PKCS#1 (RFC 2313).
- Permitir a gravação de chaves privadas e certificados digitais que utilizam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459;
- Implementar mecanismo de autenticação tipo *challenge-response*;
- Permitir a definição de política de segurança;
    - A ativação de funções que utilizem as chaves privadas só pode ser realizada após autenticação da identidade do titular do dispositivo;
    - Forçar a troca da senha padrão no primeiro acesso;
    - A utilização do dispositivo deve ser bloqueada após 5 tentativas de autenticação com códigos inválidos;
    - O titular do dispositivo deve ser avisado a cada vez que uma função que utilize sua chave privada tiver de ser ativada, e deve se autenticar para liberar a utilização pretendida;
- Possuir firewall para a proteção da memória EEPROM;
- Possuir firewall entre as áreas de memória EEPROM de cada aplicativo;
- As rotinas de criptografia, que por característica do dispositivo, manipulem as chaves privadas em memória, devem:
    - Usar área de memória do tipo non-swappable;

- Sobrescrever com valores fixos imediatamente após o término das funções que utilizaram estas chaves;
- Rodar em kernel mode, como parte do núcleo do sistema operacional, no anel 0, também chamado de "supervisor mode".

- Não permitir que a chave privada, se gerada no dispositivo, seja exportada, condicionando as transações que utilizam a chave privada a ocorrer dentro deste;

5.2.5.8. Armazenamento de chaves privadas

- As chaves privadas devem ser armazenadas em repositório de dados próprio, controlado pela solução;
- Apenas certificados pertencentes a um único titular podem ser associados às chaves contidas num determinado dispositivo;
- Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 8kbytes;
- Utilizar o algoritmo simétrico 3-DES ou AES com chaves de no mínimo 128 bits, para cifrar as chaves privadas armazenadas;
- O algoritmo simétrico 3DES deve utilizar três chaves distintas (k1, k2 e k3), geradas por derivação, a partir de um código de acesso escolhido pelo titular do repositório;
- O algoritmo simétrico AES deve ter sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório.

5.2.5.9. Plataformas suportadas

- Possuir driver disponíveis para o sistema operacional Linux kernel 2.4 e versões superiores estáveis;
- Possuir driver disponíveis para o sistema operacional Microsoft Windows 98 SE e versões superiores;
- Suportar o browser Microsoft Internet Explorer a partir da versão 5.5;
- Suportar o browser Netscape Navigator a partir da versão 7.0 ou Mozilla a partir da versão 1.3.

5.2.5.10. Gerenciamento do dispositivo

- Possuir um utilitário com interface gráfica em idioma português do Brasil, que permita gerenciamento do dispositivo;
- Permitir a exportação de certificados armazenados no dispositivo;
- Permitir a importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo de acordo com a RFC 2315;
- Permitir a importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;
- Permitir a visualização de certificados armazenados no dispositivo;
- Permitir o apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular;
- Permitir a reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso.

5.2.5.11. Certificações

- Possuir certificação CC EAL 4+ ou superior.

5.3. CARTÃO PLÁSTICO

5.3.1. Material e Durabilidade do Cartão

Alguns fatores devem ser levados em consideração na escolha de materiais, conforme suas características relativas à durabilidade dos cartões quando do projeto de um documento em smart cards.

São eles:

- Resistência a produtos químicos.
- Integridade na fabricação: adesão, coesão e laminação.
- Resistência à fadiga: Flexão.
- Resistência à abrasão.
- Resistência à umidade.

Considerando as alternativas já discutidas no capitulo 4, recomenda-se a utilização de polímeros duráveis na construção dos cartões. A exata composição do cartão será determinada pelo fabricante, porém, os cartões devem cumprir ou superar os procedimentos de teste indicados na norma NCITS 322:2002 para a durabilidade e na norma ISO/IEC 7810:1002 para resistência a produtos químicos. Os cartões submetidos aos testes devem ser previamente personalizados para que durabilidade completa do cartão seja avaliada.

5.3.2. Recomendação e especificação

Com base nos dados técnicos e na comparação dos materiais e, considerando que o uso do cartão de identidade requer alto nível de segurança e durabilidade, recomenda-se a seguinte especificação:

5.3.2.1. Dimensões do documento

Cartões utilizando suporte (plástico), em tamanho padrão ID-1 (85,6 mm por 54 mm), conforme especificado pela ISO 7810, sem tarja magnética, com chip de contato[8] embutido, em conformidade com a ISO 7816 – Partes 1 e 2.

5.3.2.2. Composição material

Composição: Cartões para identificação em material PET de alta resistência, com a seguinte composição, mostrada nas Figura 5-1 e Tabela 5-5, conforme o tempo de vida estimado que for requerido para o cartão.

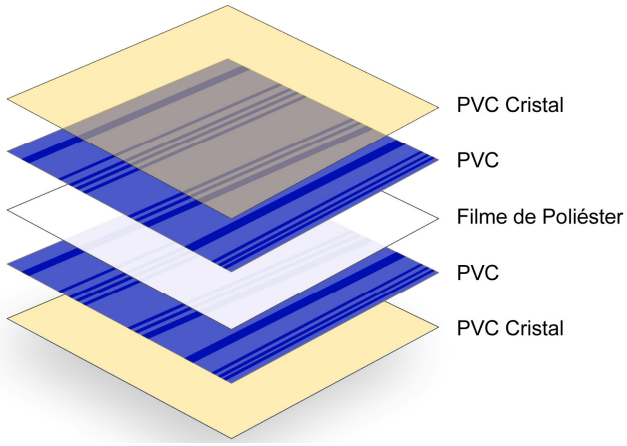


Figura 5-1 - Composição de camadas de material do cartão

[8] A especificação do chip de contato é apresentada na seção 5.2.

Esta alternativa de composição é sugerida pois o PET pode proporcionar vida útil superior ao cartão, devido às suas propriedades mecânicas. O PVC branco possui facilidade de impressão e o PVC cristal transparente é tratado para receber gravação laser. Além disso, o PVC e o PET são compatíveis para o processo de laminação, sendo que o cartão final produzido permanece com as propriedades mecânicas e térmicas dos dois materiais, alcançando vários ciclos de flexão/torção acima dos requeridos pela ISO 7810.

Tabela 5-5 - Tipos de cartões mistos

Material	Cartão Tipo I	Cartão Tipo II
Película de PET orientado de alta resistência branco opaco	20%	40%
Película de cloreto de polivinila branco opaco	60%	40%
Película de cloreto de polivinila transparente *laser engraving*	20%	20%
Vida útil prevista	Até 7 anos	Até 11 anos

5.4. REQUISITOS DE SEGURANÇA

A detecção de um item alterado em um documento requer prática. No exame de um documento é necessária a utilização de um método consistente. A segurança de um documento é avaliada baseando-se nas evidências deixadas na tentativa de fraudar um documento. É Essencial tornar essas tentativas o mais evidente possível.

A maioria dos documentos adulterados ou copiados exibe uma baixa qualidade de impressão. Uma simples comparação entre documentos suspeitos e originais frequentemente revela esses defeitos. Documentos originais têm como premissa impressões de alta qualidade. Individualmente, as letras são uniformes em tamanho, forma, estilo e espaçamento. Em falsificações as letras aparecem irregulares, quebradas ou manchadas.

Um documento seguro deve ser confeccionado com versos e fundos em padrões decorativos para ajudar a proteger a integridade dos dados impressos, uma vez que, ao se tentar modificar um dado, o padrão decorativo pode denunciar a tentativa de fraude.

Também deve trazer os requisitos de segurança dos dados eletrônicos. Criptografia e Certificação digital são itens essenciais na proteção dos dados eletrônicos. Seguem as especificações e recomendações dos requisitos de segurança dos cartões, conforme as tecnologia já descritas nos capitulo 4.

5.4.1. Itens de Segurança de Impressão Incorporados na Fabricação do Cartão Plástico.

Tabela 5-6 - Itens de Segurança de Impressão Incorporados na Fabricação do Cartão Plástico

Tipo	Item	obrigatório/ desejável/ opcional	custo adicional por cartão
Segurança gráfica nível 1	**Itens de segurança relacionados com o projeto do leiaute do cartão**		
	Linha Fina / Impressão Guilloche	obrigatório	Não
	Impressão em arco-íris ("Rainbow")	obrigatório	Não
	Modulação de Imagem (padrões de Moiré)	obrigatório	Não
	Modulação de tela	obrigatório	Não
	Erros Deliberados	obrigatório	Não
	Litografia(relevo táctil)	obrigatório	Não
	Desenhos a partir de linhas de fractais, com distorções curvas e efeitos 3D	obrigatório	Não
	Impressão intaglio (textos e imagens)	obrigatório	Não
	Impressão com Tintas Especiais de Segurança Visíveis a Olho Nu		
	Cores Customizadas, fora do padrão	desejável	Sim
	Tintas metalizadas	desejável	Sim
	Tintas peroladas	desejável	Sim
	Tintas "Iridescent"	desejável	Sim
	Dispositivos Opticamente Variáveis		
	Dispositivos Iridescent		
	ISIS (light Interference Security Image Structures)		
	Retro reflexivo (3M Confirm™)	desejável	Sim
	Advantage™	opcional	Sim
	Indentiseal™	opcional	Sim
	DOVID: Diffractive Optically Variable Image Device		
	Holograma em duas dimensões	desejável	Sim
	Holograma em três dimensões	opcional	Sim
	Cinegramas	opcional	Sim
	Dispositivos "Non-Iridescent"		
	Perfuração a laser	opcional	Sim
	Imagens cauterizadas	opcional	Sim
	Imagens inclinadas a laser	opcional	Sim

Tabela 5-6 - Itens de Segurança de Impressão Incorporados na Fabricação do Cartão Plástico

Tipo	Item	obrigatório/ desejável/ opcional	custo adicional por cartão
	Imagens latentes	desejável	Sim
Segurança gráfica nível 2	**Micro Impressão**		
	Micro Impressão (texto)	obrigatório	Não
	Micro impressão (imagens)	obrigatório	Não
	Variações na espessura da linha	obrigatório	Não
	Impressão com tintas especiais de segurança invisíveis a olho nú		
	Tintas Ultra Violeta (UV)		
	Tintas para UV em baixas freqüências	obrigatório	Sim
	Tintas para UV em altas freqüências	obrigatório	Sim
	Tintas Infravermelho (IR)		
	Tintas fluorescentes	desejável	Sim
	Tintas absorventes	desejável	Sim
	Tintas "Metameric"	desejável	Sim
	Tecnologias usando imagens geradas por computador		
	Dataglyph™	desejável	Sim
	Digimarc™	opcional	Sim
	Quilt™	opcional	Sim
	Scrambled Indicia™	desejável	Sim
	Copy Ban™	opcional	Sim
	Microbar™	opcional	Sim
	SafeCopyVoid™	desejável	Sim

Tabela 5-6 - Itens de Segurança de Impressão Incorporados na Fabricação do Cartão Plástico

Tipo	Item	obrigatório/ desejável/ opcional	custo adicional por cartão
Segurança gráfica nível 3	Tintas inteligentes	desejável	Sim
	Materiais ocultamente embutidos		
	Óptico (assinaturas de luz)		
	Copytex	opcional	Sim
	Fibras de polímeros	opcional	Sim
	Magnético		
	NHK	opcional	Sim
	MagnaPrint	opcional	Sim
	RF		
	Bakeart	opcional	Sim
	Inkode	opcional	Sim
	Marcas moleculares: Isotag	opcional	Sim
	Microtaggants	opcional	Sim
Auditoria	Número de Série	obrigatório	Não

5.4.2. Itens de Segurança de Impressão de Dados Variáveis (Personalização)

5.4.2.1. Opção 1: Fotografia em preto-e-branco com laser engrave

Tabela 5-7 - Itens de segurança de impressão de dados variáveis (personalização) - opção com foto preto e branco em laser engrave

Item	**obrigatório/ desejável/ opcional**	**custo adicional por cartão**
Dados redundantes	obrigatótio	Não
Dados Sobrepostos	obrigatótio	Não
Imagem Fantasma - visível	opcional	Não
Imagem Fantasma - invisível (UV)	desejável	Sim
Erros deliberados	desejável	Não
Padrões de segurança no campo (caixa) de fotografia	desejável	Não
Impressão de dados variáveis e foto com laser engrave	obrigatótio	Não
Impressão de texto com tinta ultravioleta (UV)	desejável	Sim
Impressão de texto com fontes pequenas	obrigatótio	Não
Capa de proteção		
Lâmina holográfica	desejável	Sim
Lâmina perolada	opcional	Sim
Lâmina com impressão em UV	opcional	Sim
Conversão de dados dentro de imagens		
Scrambled Indicia™	opcional	Sim
Digimarc™	opcional	Sim

5.4.2.2. Opção 2: Fotografia colorida

Tabela 5-8 - Itens de segurança de impressão de dados variáveis (personalização) - opção com foto colorida

Item	obrigatório/ desejável/ opcional	custo adicional por cartão
Dados redundantes	obrigatótio	Não
Dados Sobrepostos	obrigatótio	Não
Imagem Fantasma - visível	opcional	Não
Imagem Fantasma - invisível (UV)	desejável	Sim
Erros deliberados	desejável	Não
Padrões de segurança no campo (caixa) de fotografia	desejável	Não
Impressão de dados variáveis com laser engrave	obrigatótio	Não
Impressão de foto colorida (jato de tinta)	obrigatótio	Sim
Impressão de texto com tinta ultravioleta (UV)	desejável	Sim
Impressão de texto com fontes pequenas	obrigatótio	Não
Capa de proteção		
Lâmina holográfica	obrigatória	Sim
Lâmina perolada	opcional	Sim
Lâmina com impressão em UV	opcional	Sim
Conversão de dados dentro de imagens		
Scrambled Indicia™	opcional	Sim
Digimarc™	opcional	Sim

5.4.3. Segurança Eletrônica Implementada no Chip (Criptografia)

5.4.3.1. Algoritmos criptográficos suportados pelo chip

- Cenário 1
  - Criptografia simétrica.
  - Funções de hash.
- Cenários 2 e 3:
  - Criptografia simétrica.
  - Criptografia assimétrica.
  - Funções de hash.
  - Assinatura digital.

5.4.3.2. Autenticação e confidencialidade dos dados armazenados no cartão

- Assinatura digital dos dados armazenados no cartão: Assinatura digital dos dados armazenados no cartão, usando SHA1 e RSA, através de protocoladora digital.
- Criptografia de dados transferidos do cartão para a aplicação: Criptografia (simétrica) dos dados na comunicação.

5.4.4. Certificado Digital Pessoal

- Este item é viável apenas nos cenários 2 e 3.
- Recomenda-se a utilização de cartificados pessoais do tipo A3 (ICP Brasil), com chaves RSA de, no mínimo, 1024 bits. O certificado deverá ser armazenado e gerenciado internamento no smart card.
- O acesso à chave privada deverá ocorrer apenas mediante apresentação de PIN (senha).
- Operações criptográficas com a chave privada deverão ser realizadas exclusivamente no smart card.

5.4.5. PCC (Proof-carrying code)

- Este item é viável apenas no cenário 3.
- Deve ser definido em função da política de segurança.

6. CONCLUSÕES

Este trabalho apresenta uma proposta tecnológica para a concepção de um documento de identidade eletrônica para o Brasil, tendo como premissa a adoção de cartões inteligentes como mídia de suporte para o novo documento. Ainda que a avaliação dessa premissa não conste como escopo deste trabalho, tal escolha é fundamentada na análise de tendências mundiais e de experiências bem sucedidas em outros países.

A tecnologia de smart cards está em constante evolução e sua disponibilização se dá em um mercado globalizado e extremamente competitivo. Nestes casos, é comum a adoção de padrões internacionais que regulam o desenvolvimento de tecnologias colocadas no mercado, visando assegurar um nível mínimo de independência para com fornecedores específicos para os usuários através da interoperabilidade entre produtos de diferentes fornecedores. Ainda que existam diversas normas e padrões internacionais regulando o desenvolvimento da tecnologia de smart cards e mesmo a tecnologia de e-ID este estudo mostra que tais definições ainda são insuficientes para assegurar uma completa interoperabilidade entre os diversos produtos existentes no mercado. Desse modo, é necessário um cuidado especial com aspectos de portabilidade e disponibilidade de recursos no mercado quando da definição do novo e-ID brasileiro, sob pena de se ficar refém deste ou daquele fornecedor de tecnologia. Assim também, se faz necessário o acompanhamento constante da evolução das normas e das tecnologias, uma vez que o aperfeiçoamento da segurança de documentos é um processo contínuo de avaliação de tecnologias disponíveis e no estado da arte.

Existem diversas alternativas tecnológicas e possibilidades de uso de um documento de identificação eletrônica. Este trabalho procurou abordar os principais aspectos relacionados à tecnologia de documentos e tem como contribuição mais saliente a proposição de elementos técnicos para composição de um documento de identificação alinhados com as possibilidades de uso desse documento.

Os estudos realizados mostram que não há uma abordagem única e consensual para a definição de um documento de identificação eletrônica para o Brasil, em especial porque tal definição depende do estabelecimento de uma política de uso para o

documento. Desse modo, a elaboração dessa política deve preceder a especificação precisa do tipo de chip, plástico e elementos de segurança adotados no novo documento. Como essa política não está disponível, foram analisados cenários de uso e define-se um conjunto de requisitos técnicos para cada cenário, com objetivo de reunir informações sobre as alternativas tecnológicas e o seu significa para cada tipo de uso do documento.

Por fim, fica claro que não existe um único projeto para um documento de identificação seguro e sim uma gama de opções que devem ser customizadas caso a caso. A necessidade de planejamento dos processos de segurança física e da cadeia produtiva fica proposto para estudos futuros e serão complementares a essa dissertação.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] A. K. Jain, L. Hong, S. Pankanti, R. Bolle, 1997. An identity authentication system using fingerprints, Proceedings of the IEEE, 85(9) 1365-1388.

[2] A. Moenssens. Fingerprint Techniques. Chilton Book Company, London, 1971

[3] ALLEN, C.; BARR, W. Smart Cards. ediçao. [S.l.: s.n.], 1997.

[4] ANSI INCITS 358-2002 – The Biometric API, Feb 2002.

[5] ANSI INCITS 378-2004, American National Standard for Information Technology - Finger Minutiae Format for Data Interchange.

[6] ANSI INCITS 381-2004, American National Standard for Information Technology - Finger Image-Based Data Interchange Format

[7] B. Bhanu, M. Boshra, Tan, 2000. Logical templates for feature extraction in fingerprint images, Proc. Int'l. Conf. on Parrern Recognition (ICPR), Barcelona, Spain, Sepember, Vol III, pp. 850-854.

[8] B. Bhanu, X. Tan, 2001. Learned template for feature extraction in fingerprint images, Proc. IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), Vol. II, Hawaii, USA, pp. 591-596.

[9] B. M. Mehtre, B. Chatterje, 1989. Pattern Recognition, 22, 4, pp 381-385.

[10] B. Moayer and K.S. Fu , A Syntactic Approach to Fingerprint Pattern Recognition, Pattern Recognition, v. 7, pp. 1--23, 1975.

[11] BETTS, E. O mercado de Smart Card na América Latina. http://www.iti.br/twiki/pub/Main/PalesCart2006/EDGARCertForumJointPresentationwithITI-Final2.pdf, Novembro 2006.

[12] Biometric Market Report 2003–2007. http://www.kiosks.org/pdfs/BMR_2003-2007.pdf . Acessado em 04 abr. 2005.

[13] D. A. Stoney, 1988. Distribution of epidermal ridge minutiae, American Journal of Physical Anthropology 77, pp 367-376.

[14] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, Springer (New York), 2003.

[15] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, Springer (New York), 2003.

[16] D.C.D. Hung, 1993. Enhancement and feature purification of fingerprint images, Pattern Recognition, 26(11) 1,661-1,671.

[17] E. Newham. The Biometric Report. SJB Services, New York, 1995

[18] EC 2252/2004 – Concil Regulation on standards for security features and biometrics in passports and travel documents issued by Member States, European Union, Dec 2004.

[19] EUR 21585 EN - Biometrics at the Frontiers: Assessing the Impact on Society, European Comission, Institute for Prospective Technological Studies, Feb 2005.

[20] EUROSMART. EUROSMART, The Voice of the Smart Card Industry. http://www.eurosmart.com, Novembro 2006.

[21] F. Galton, Finger Prints, McMillan, London, 1892.

[22] Federal Identity Management Handbook, US General Service Administration, March 2005.

[23] Feu vert pour la carte d'identité électronique - LE MONDE 12.04.05.

[24] FINKENZELLER, K. RFID Handbook. 2. ed. [S.l.], 2003.

[25] FIPS Publication 201, Federal Personal Identity Verification (PIV) for Federal Employees and Contractors (Feb. 25, 2005).

[26] GARTNER. 2004 Documento de Reference. http://www.axalto.com/Company/Financial/pdf/2004ReferenceDocument.pdf, Novembro 2006.

[27] H.C. Lee and R.E. Gaensslen. Advances in Fingerprint Technology, 2nd ed. Elsevier, New York, 2001.

[28] ICAO 9303 part 3 : 2002 [icao] machine readable travel documents - size 1 and size 2 machine readable official travel documents.

[29] ICAO Technical Report - Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents, May, 2004.

[30] INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. ICP-Brasil. http://www.icpbrasil.gov.br, Novembro 2006.

[31] ISO 1073-2 : 1976 alphanumeric character sets for optical character recognition – part 2: character set ocr-b – shapes and dimensions of the printed image.

[32] ISO 1831 : 1980 printing specifications for optical character recognition.

[33] ISO 3166-1: 1997 codes for the representation of names of countries and their subdivisions – part 1: country codes.

[34] ISO 8601 : 2001 data elements and interchange formats – information interchange – representation of dates and times.

[35] ISO/IEC 10646-1 character set unicode [ITRSS] security standards for machine readable travel documents, technical.

[36] ISO/IEC 7501-3: 1997 machine readable travel documents – identity cards.

[37] ISO/IEC 7810 : 1995 identification cards – physical characteristics.

[38] ISO/IEC 7812-1: 2000 identification cards – identification of issuers – numbering system.

[39] J. C. Amengual, A. Juan, J. C. Perez, et. al. 1997. Real-time Minutiae Extraction in Fingerprint Images.

[40] JPEG 2000 ISO 15444, Information Technology - Digital Compression and Coding of Continuous-Tone Still Images

[41] JPEG 2000 Part 5 (ISO/IEC 15444-5:2003) http://www.jpeg.org/jpeg2000/j2kpart5.html

[42] L. Hong, Y. Wan, A. K. Jain, 1998. Fingerprint image enhancement: algorithm and performance evaluation, IEEE Trans. Pattern Analalysis and Machine Intelligence, 20(8) 777-789.

[43] L. Hong. Automatic Personal Identification Using Fingerprints. 1998. 242 f. Dissertação (Doutorado em Filosofia) – Dep. Ciências da Computação, Michigan State University. Disponível em: http://www.cse.msu.edu/publications/tech/TR/MSU-CPS-98-24.ps.gz. Acessado em 04 abr. 2005.

[44] L. O'Gorman, J.V. Nickerson, 1989. An approach to fingerprint filter design, Pattern Recognition, 22, 1, pp 29-38.

[45] MANUAL de Condutas Técnicas. [S.l.], Julho 2006.

[46] National Center For Electron Microscopy. FIB. http://ncem.lbl.gov/frames/FIB.html, Dezembro 2006.

[47] NIST Special Publication 800-73, Interfaces for Personal Identity Verification.

[48] NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification.

[49] NIST Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification.

[50] NISTIR 6529 - The Common Biometric Exchange File Format (CBEFF), Jan 2001.

[51] NISTIR 6529-2001, Common Biometric Exchange File Format

[52] OLIVEIRA, W. Segurança da Informação - Técnicas e Soluções. 1. ed. [S.l.]: Centro Atlântico.PT, 2001.

[53] Optical Document Security, 2nd edition, R.L. van Renesse, editor, Publisher Artech House (Boston/London) 1998.

[54] PARDAL, M. F. L. Interoperabilidade de cartões inteligentes. [S.l.], Julho 2004.

[55] PERTO S/A. Perto S/A - Periféricos para automação. http://www.perto.com.br, Novembro 2006.

[56] Q. Xiao and H. Raafat, Fingerprint Image Post-processing: A Combined Statistical and Structural Approach, Pattern Recognition, vol. 24, no. 10, pp. 985-992, Oct. 1991.

[57] R. M. Bolle, A. W. Senior, N. K. Ratha, et. al. 1998, Fingerprint Minutiae: A Constructive Definition, Lecture Notes in Computer Science

[58] RANKL, W.; EFFING, W. Smart Card Handbook. 3. ed. [S.l.], 2004.

[59] Report, ICAO SS 614314 identification card – identity card of type id-1, (identifieringskort – identitetskort av typ ID-1).

[60] Resolution of the representatives of the governments of the member states, meeting within the council of 17 october 2000 supplementing the resolutions of 23 june 1981, 30 june 1982, 14 july 1986 and 10 july 1995 as regards the security characteristics of passports and other documents. Official journal c 310,28/10/2000 p. 0001.

[61] Rudolf L. van Renesse, "Ordering the Order - A survey of optical document security features," SPIE Conference on Practical Holography IX, San Jose, California.

[62] Rudolf L. van Renesse, "Paper Based Document Security - A Review", European Conference on Security and Detection, Comonwealth Institute, London. 28-30 April 1997.

[63] S. Prabhakary, A. K. Jain, S. Pankanti, 2000. Learning Fingerprint Minutiae Location and Type, 15th International Conference on Pattern Recognition (ICPR), Barcelona, September 3-8

[64] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino. Impact of Artificial "Gummy" Fingers on Fingerprint Systems, Proceedings of of SPIE Vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

[65] Wolfgang Rankl and Wolfgang Effing, Smart Card Handbook 2nd Edition, John Wiley & Sons, 2000.

[66] Zhiqun Chen, Java Card Technology for Smart Cards: Architecture and Programmer's Guide (The Java Series), Addison-Wesley, 2000.