Infra-Estrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 2 - Volume I

Requisitos, Materiais e Documentos Técnicos para Homologação de Leitoras de Cartões Inteligentes no Âmbito da ICP-Brasil

versão 3.0

São Paulo, 22 de novembro de 2007

Sumário

Controle de Versão

Versão atual	Data de emissão	Alterações realizadas
2.0.r.6	**07/06/06**	Revisões de ambiente operacional (seção 2.1.6) Revisões de classe de operação para cartão e leitora (seção 3.5 REQUISITO III.20). Revisão das funcionalidades do papel de acesso "usuário" (seção 2.2.12 REQUISITO II.21). Inclusão do termo "Módulo criptográfico multiaplicação" no glossário.
3.0.r.50	**22/11/07**	Revisão geral para os requisitos de cartões criptográficos ICP e leitoras de cartões inteligentes. Exclusão dos requisitos de *tokens* criptográficos. Revisão estrutural do Manual de Condutas Técnicas incluindo no desenvolvimento do mesmo documento os requisitos técnicos para cartões criptográficos ICP, leitoras de cartões inteligentes e materiais a serem depositados para a execução do processo de homologação.

Listas de Ilustrações

Lista de Figuras

Lista de Tabelas

1 Introdução

Este documento descreve os requisitos técnicos a serem observados no processo de homologação de leitora de cartões inteligentes no âmbito da Infra-Estrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Para uma melhor compreensão do disposto neste documento, entenda-se por leitora de cartão inteligente um hardware instalado no computador que utiliza uma conexão física do tipo Serial (RS232) ou USB, que serve de interface de interação entre o cartão inteligente e uma aplicação.

1.1 Objetivo da homologação

O objetivo do processo de homologação de leitora de cartões inteligentes é propiciar a interoperabilidade e operação segura de leitora de cartões inteligentes por meio da avaliação técnica de aderência aos requisitos técnicos definidos neste manual.

1.2 Descrição do processo de homologação

O processo de homologação é baseado em um conjunto de requisitos técnicos definidos neste manual que devem ser atendidos por uma leitora de cartões inteligentes para prover interoperabilidade e operação segura.

Estes requisitos técnicos são avaliados pela execução de ensaios de aderência aos requisitos técnicos. Para a realização destes ensaios, a parte interessada deve submeter ao processo de homologação um conjunto de materiais requisitados, efetuando o depósito destes materiais no LEA.

1.3 Escopo deste manual

O escopo dos requisitos técnicos e da avaliação de leitoras de cartões inteligentes se aplicam aos seguintes componentes:

- Componentes da leitora de cartão inteligente, incluindo:
  - Componentes eletrônicos;
  - componentes mecânicos;
  - firmware e softwares embarcados;

- componentes de entrada de dados (quando suportado) como, por exemplo, PIN pad e dispositivos biométricos;
- interface de comunicação;
- driver (software de controle) da leitora.

O resultado do processo de homologação de leitoras de cartões inteligentes informa a aderência aos requisitos técnicos definidos neste manual.

1.4 Estruturação do MCT 2 – Volume I

Este documento (MCT 2 – Volume I) está estruturado da seguinte forma:

- Parte 1: Descreve os requisitos técnicos que devem ser verificados no processo de homologação de leitoras de cartões inteligentes;
- Parte 2: Descreve os materiais que devem ser depositados para a execução do processo de homologação de leitoras de cartões inteligentes;
- Referência Bibliográfica: Descreve as referências bibliográficas que foram utilizadas na elaboração deste documento.

2 Parte 1

Requisitos técnicos a serem observados no processo de homologação de leitoras de cartões inteligentes no âmbito da ICP-Brasil

2.1 Introdução

Esta parte apresenta os requisitos técnicos que devem ser verificados no processo de homologação de leitoras de cartões inteligentes.

Os requisitos técnicos descritos nesta parte englobam:

- Recomendações de segurança;
- requisitos de interoperabilidade;
- requisitos de documentação.

2.2 Recomendações de segurança

As recomendações de segurança descrevem mecanismos de segurança adicionais que podem estar implementados em leitoras de cartões inteligentes com a finalidade de proteger dados críticos de identificação e autenticação da entidade usuária externa pela leitora, como por exemplo, o PIN. Mecanismos de segurança adicionais implementados em leitoras de cartões inteligentes podem ser:

- Teclado numérico isolado (PIN *pad*) para a entrada de dados numéricos que serão enviados ao cartão inteligente para fins de identificação e autenticação da entidade usuária externa;
- teclado alfanumérico isolado para a entrada de dados alfanuméricos que serão enviados ao cartão inteligente para fins de identificação e autenticação da entidade usuária externa;
- dispositivo biométrico isolado para fins de identificação e autenticação da entidade usuária externa no cartão inteligente;
- tela (*display*) isolada para a apresentação de dados críticos de segurança que são gerados pelo cartão inteligente.

REQUISITO I.1: Caso a leitora de cartões inteligentes suporte mecanismos de segurança adicionais, então o envio de dados críticos de segurança ao cartão inteligente para fins de identificação e autenticação da entidade usuária externa deve estar sob controle exclusivo da leitora.

REQUISITO I.2: A documentação técnica deve descrever os mecanismos de segurança que estejam implementados na leitora, incluindo:

- Algoritmos criptográficos e protocolos utilizados para troca segura de informações entre o dispositivo de entrada (PIN pad, teclado alfanumérico ou dispositivo biométrico) e o cartão inteligente;

- mecanismos de cachê de dados de autenticação;
- realimentação de dados de autenticação (*echo*) para uma entidade usuária externa de forma obscura durante a autenticação (por exemplo, nenhuma exibição legível de caracteres no momento da inserção de um PIN);
- mecanismos utilizados para que dados de autenticação manipulados pela leitora estejam protegidos contra leitura não autorizada;
- mecanismos de segurança física utilizados para previnir acesso físico não autorizado aos componentes da leitora;
- mecanismos que mitigam ataques, como por exemplo, proteção contra vazamento de informações por emanações eletromagnéticas (*Electromagnetics Attacks – EMA*) ou por consumo de corrente (*Differential Power Analysis – DPA*).

2.3 Requisitos de Interoperabilidade

REQUISITO II.1: Leitoras de cartões inteligentes, sempre que aplicável a cada caso, devem atender aos requisitos de interoperabilidade ora estabelecidos, derivados e complementares aos padrões ISO/IEC 7816 e PS/SC versão 1.0, conforme descrito nos itens a seguir.

2.3.1 Interface física entre leitoras e cartões inteligentes

Esta seção determina os requisitos de interoperabilidade e compatibilidade que devem ser atendidos por leitoras e cartões inteligentes no que diz respeito a interface física entre eles. Tais requisitos foram derivados dos padrões ISO/IEC 7816-2 e PC/SC versão 1.0, a saber:

- *Interoperability Specification for ICCs and Personal Computer Systems - Part 2*. "*Interface Requirements for Compatible IC Cards and Readers*";
- ISO/IEC 7816-2 *Identification cards – Integrated circuit(s) cards with contacts – Part 2*: *Dimensions and location of the contacts* – ISO/IEC 7816-2.

2.3.1.1 Requisitos de interface física

2.3.1.1.1 Atribuição de contatos elétricos

REQUISITO II.2: Os contatos elétricos localizados em uma leitora de cartões inteligentes devem ser compatíveis com os requisitos definidos na seção 5 do padrão ISO/IEC 7816-2 e identificados conforme mostra a Tabela 1.

Tabela 1. Identificação dos contatos para leitoras de cartões inteligentes

Identificação do contato	Descrição
C1	Voltagem de alimentação (s*upply voltage* – Vcc)
C2	Sinal "reset" (RST)
C3	Sinal "clock" (CLK)
C4	Reservado para uso futuro em outras partes do ISO/IEC 7816 (não usado atualmente) - RFU (r*eserved for future use*)
C5	terra – "ground" (GND)
C6	Identificado pelo padrão ISO/IEC 7816-2 como "voltagem de programação" (v*ariable supply voltage* - VPP) – geralmente não mais usado
C7	entrada/saída de dados (d*ata input*/*output* – I/O)
C8	reservado para uso futuro em outras partes do ISO/IEC 7816 (não usado atualmente) - RFU (r*eserved for future use*)

OBSERVAÇÃO: Para leitoras de cartões inteligentes, os contatos elétricos C4, C6 e C8 podem ser considerados opcionais. Entretanto, para fins de compatibilidade com alguns tipos de cartões inteligentes, alguns destes contatos podem ser utilizados possuindo, como por exemplo, a finalidade de fornecer uma alimentação auxiliar para cartões de memória.

REQUISITO II.3: Caso os contatos C4, C6 e C8 não sejam necessários, então devem estar isolados, do ponto de vista elétrico (não condutíveis), dos circuitos integrados e de quaisquer outros contatos inseridos na leitora. Caso os contatos C4, C6 ou C8 sejam utilizados para uma finalidade específica, a documentação técnica deve descrever a finalidade de uso e características dos respectivos contatos.

REQUISITO II.4: Os contatos elétricos da leitora de cartões inteligentes devem seguir as disposições definidas na seção 4 da ISO 7816-2, conforme apresentado na Figura 1.

C1	C5	Vcc	GND
C2	C6	RST	Vpp
C3	C7	CLK	I/O
C4	C8	RFU	RFU

Figura 1. Numeração dos contatos elétricos para leitoras de cartões inteligentes segundo padrão ISO 7816-2

REQUISITO II.5: A documentação técnica deve descrever a identificação dos contatos elétricos presentes na leitora de cartões inteligentes.

2.3.1.1.2 Inserção e remoção de cartões inteligentes

As recomendações e requisitos descritos a seguir devem ser atendidos por leitoras que usam mecanismos de inserção e remoção manuais.

RECOMENDAÇÃO II.1: É recomendado que leitoras sejam projetadas para posicionar cartões inteligentes de tal forma que sempre estejam acessíveis por seus respectivos proprietários.

RECOMENDAÇÃO II.2: Para facilitar a popularização deste tipo de dispositivo, é recomendado que leitoras tenham mecanismos manuais simples de inserção e remoção de cartões inteligentes.

REQUISITO II.6: Leitoras devem assegurar que quaisquer objetos ou materiais físicos, tais como, mas não limitados a sinais indicativos, grampos, parafusos, braçadeiras, pinças, rolos e cilindros, não danifiquem um cartão inteligente, particularmente nas áreas reservadas para tarjas magnéticas e saliências de identificação do proprietário.

REQUISITO II.7: A documentação técnica deve descrever quais mecanismos de inserção e remoção de cartões inteligentes são suportados pela leitora.

REQUISITO II.8: Quando aplicável, a documentação técnica deve especificar quais mecanismos de inserção e remoção de cartões inteligentes são suportados pela leitora.

2.3.2 Propriedades elétricas

Em conformidade com o padrão ISO/IEC 7816-3, duas classes de operação são definidas para representar a voltagem de alimentação (Vcc) aplicada por leitoras em cartões inteligentes:

- Classe A: 5V;
- classe B: 3V.

Além disso, existem outros requisitos técnicos relacionados às propriedades elétricas entre leitoras e cartões inteligentes:

- Método de seleção da classe de operação executado pela leitora;
- valores definidos com relação à voltagem e corrente elétrica.
- freqüência de operação;

REQUISITO II.9: Uma leitora de cartões inteligentes deve atender aos requisitos de propriedades elétricas definidos na seção 4 do padrão ISO/IEC 7816-3. Para leitora de cartões inteligentes, no mínimo, a classe de operação A deve ser suportada.

REQUISITO II.10: A documentação técnica da leitora deve descrever qualquer propriedade elétrica suportada que seja adicional ou não compatível aos requisitos definidos na seção 4 do padrão ISO/IEC 7816-3.

2.3.3 Transferência de dados em cartões inteligentes

A comunicação com um cartão inteligente é sempre iniciada pela leitora. Desta forma, um cartão inteligente sempre responde a comandos da leitora, nunca enviando dados sem qualquer requisição. Este tipo de relação é denominada de “mestre e escravo”, sendo que a leitora desempenha o papel de mestre e o cartão inteligente desempenha o papel de escravo.

Depois que um cartão inteligente for inserido em uma leitora, seus contatos elétricos são mecanicamente conectados aos da leitora. Portanto, os circuitos elétricos da leitora não devem ser ativados até que os contatos do cartão inteligente estejam mecanicamente conectados aos contatos da leitora.

A interação entre a leitora e o cartão inteligente deve ser conduzida por meio das seguintes operações consecutivas:

- Ativação: corresponde à ativação dos circuitos elétricos por parte da leitora;
- troca de informações: corresponde à troca de informações entre cartão inteligente e leitora, sendo que o cartão sempre responde ao estímulo de reinício (*reset*) feito previamente pela leitora;
- desativação: corresponde à desativação dos circuitos elétricos por parte da leitora, devido, por exemplo, à retirada do cartão inteligente.

REQUISITO II.11: A leitora deve atender aos requisitos de ativação dos circuitos elétricos (*cold reset*) definidos na seção 5.3.2 do padrão ISO/IEC 7816-3 .

REQUISITO II.12: A leitora deve atender aos requisitos de ativação a quente dos circuitos elétricos (*warm reset*) definidos na seção 5.3.3 do padrão ISO/IEC 7816-3 .

REQUISITO II.13: A leitora deve atender aos requisitos de desativação dos circuitos elétricos (*desactivation*) definidos na seção 5.4 do padrão ISO/IEC 7816-3 .

2.3.3.1 ATR

DEFINIÇÃO: Com base no padrão ISO/IEC 7816-3, seção 6, subseção 6.1, o ATR (*Answer To Reset*) é o valor da seqüência de bytes enviado pelo cartão inteligente à leitora como resposta ao estímulo de reinício (*reset*) . Neste caso, cada byte é transportado em um caractere assíncrono.

Portanto, conforme mostra a Figura 2, cada estímulo de reinício (*reset*) bem sucedido deve resultar em uma resposta ATR por parte do cartão inteligente. Caso seja necessário fixar alguns parâmetros de transferência de dados que dizem respeito ao protocolo do cartão, uma requisição PPS (*Protocol and Parameters Selection*) pode ser utilizada. Caso contrário, a leitora analisa o ATR contendo vários parâmetros relacionados ao cartão e à transferência dos dados, e depois envia o primeiro comando a ser processado.

Segundo o padrão ISO/IEC 7816-3, a configuração de um ATR é formada pelos seguintes elementos:

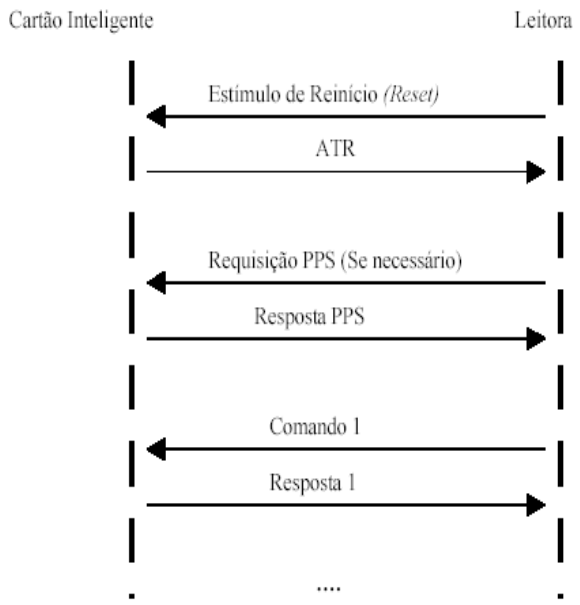

Figura 2. Transferência de dados entre leitora e cartão inteligente

- TS: Caractere inicial;
- T0: Caractere de formato;
- TA(i), TB(i), TC(i) e TD(i): Caracteres de interface;
- T1, T2, ..., TK: Caracteres históricos;
- TCK: Caractere de verificação.

Segundo o padrão ISO/IEC 7816-3, a configuração de uma sequência PPS é formada pelos seguintes elementos:

- PPSS: Caractere inicial;
- PPS0: Caractere de formato
- PPS1, PPS2, PPS3: Caracteres de parâmetro
- PCK: Caractere de verificação

REQUISITO II.14: Leitora de cartões criptográficos ICP devem atender aos requisitos de ATR e PPS de acordo com o padrão ISO/IEC 7816-3 (seções 6 e 7).

2.3.3.2 Protocolos de transmissão de dados

A comunicação com um cartão inteligente pode ser implementada de diversas maneiras por meio de protocolos de transmissão de dados envolvendo o envio de comandos, as respectivas respostas e procedimentos usados quando da ocorrência de erros de transferência de dados.

De acordo com o padrão ISO/IEC 7816-3, há um total de 15 protocolos de transmissão definidos para permitir a comunicação com cartões inteligentes, a saber:

- T=0: faz referência à transmissão assíncrona do tipo "*half-duplex*" orientada a caracteres;
- T=1: faz referência à transmissão assíncrona do tipo "*half-duplex*" orientada a blocos;
- T=2 e T=3: reservados para operações futuras do tipo "*full-duplex*";
- T=4: reservado para uma transmissão assíncrona do tipo "*half-duplex*" e também orientada a caracteres, representando uma versão estendida do protocolo T=0;
- T=5 a T=13: reservados para uso futuro;
- T=14: faz referência aos protocolos de transmissão não padronizados pelo ISO/IEC JTC 1 SC 17 (em alguns casos, T=14 é usado para atender funções nacionais);
- T=15: não faz referência a um protocolo de transmissão, mas, de acordo com o padrão ISO/IEC 7816-3 (seção 6), somente qualifica bytes de interface global.

Destes protocolos de transmissão definidos pelo padrão ISO/IEC 7816-3, dois deles são mais usados em âmbito internacional: T=0 e T=1.

REQUISITO II.15: Uma leitora de cartões inteligentes deve atender aos requisitos de protocolo de transmissão T=0 definidos pelo padrão ISO/IEC 7816-3 (seção 8).

REQUISITO II.16: Uma leitora de cartões inteligentes deve atender aos requisitos de protocolo de transmissão T=1 definidos pelo padrão ISO/IEC 7816-3 (seção 9).

REQUISITO II.17: A documentação técnica da leitora deve descrever os protocolos de transmissão suportados em conformidade com o padrão ISO/IEC 7816-3 seções 8 e 9.

2.3.4 Conexão de leitoras em computadores pessoais

Esta seção detalha os requisitos de interoperabilidade que devem ser atendidos por leitoras de cartões inteligentes quando conectadas em computadores pessoais (PC – *Personal Computers*). Tais requisitos foram derivados do padrão PC/SC versão 1.0, de dezembro de 1997, a saber:

- *Interoperability Specification for ICCs and Personal Computer Systems - Part 3*. "*Requirements for PC-Connected Interface Devices*";
- *Interoperability Specification for ICCs and Personal Computer Systems - Part 4*. "*IFD Design Considerations and Reference Design Information*".

Os requisitos de interoperabilidade necessários para uma leitora estão concentrados em três componentes (veja Figura 3):

- Leitora: dispositivo físico que provê a interface com um cartão inteligente;
- driver de Leitora: corresponde a um driver instalado no PC que permite ao sistema operacional e outros componentes de software se comunicarem com a leitora (dispositivo de hardware);
- módulo de Interface: corresponde à interface de programação hospedada em um PC que realiza interações entre o componente "Driver de Leitora" e as camadas superiores.

Portanto, conforme ilustrado na Figura 3, esta seção restringe seu escopo em especificar requisitos de interoperabilidade que estão relacionados a:

- Leitora;
- driver de leitora;
- módulo de interface;
- funcionalidades do módulo de interface.

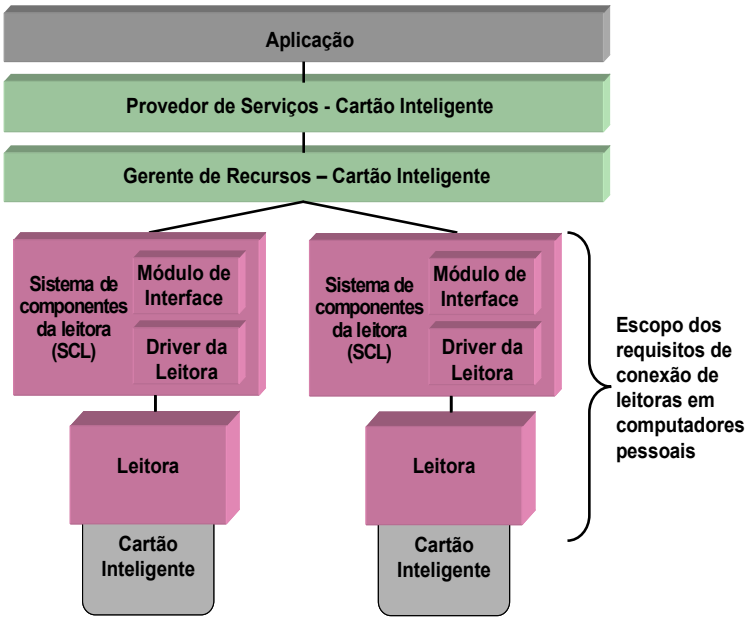

Figura 3. Componentes de leitoras que devem atender aos requisitos de interoperabilidade especificados

2.3.4.1 Leitora

REQUISITO II.18: A leitora se conecta a um PC como um dispositivo periférico devendo atender aos seguinte requisitos:

- Suportar comunicações de dados bidirecionais entre um cartão inteligente e um PC;
- incorporar as funcionalidades necessárias para suportar a interface disponível pelo componente “módulo de interface”.

2.3.4.2 Driver Leitora

REQUISITO II.19: Com relação ao canal de entrada e saída de dados (I/O) em um PC, pelo menos, uma das seguintes interfaces deve ser suportada pela leitora e seu respectivo driver:

- PS/2 (interface integrada ao teclado);
- RS-232 (interface do tipo porta serial);
- placa com interface adaptada;
- interface do tipo porta paralela;
- interface de PC baseada em cartão externo (PCMCIA de computadores portáteis (*laptops*), por exemplo);

- interface SCSI;
- interface USB.

RECOMENDAÇÃO II.3: Considerando leitoras de cartões inteligentes com interface USB, é recomendado, para fins de interoperabilidade, a implementação do padrão USB CCID Revisão 1.1 [CCID 1.1].

2.3.4.3 Módulo de interface

O módulo de interface corresponde a um software sendo executado em um PC que implementa uma interface padrão e independente tanto do hardware quanto do canal de I/O. Além disso, o módulo de interface também deve mapear as funcionalidades disponíveis pela leitora.

REQUISITO II.20: A parte interessada possui a responsabilidade de criar os componentes "driver de leitora" e "módulo de interface", de tal forma que seja possível aos SPs (*Service Providers*) se comunicarem com um cartão inteligente por meio da leitora.

REQUISITO II.21: Drivers de leitoras de cartões inteligentes devem prover mecanismos de tratamento de erros.

2.3.4.4 Funcionalidades do módulo de interface

As funcionalidades descritas a seguir estão relacionadas aos requisitos de interoperabilidade, e devem estar visíveis por meio do componente "módulo de interface".

2.3.4.4.1 Funcionalidades obrigatórias

A - Características Operacionais

REQUISITO II.22: Em um dado instante, o módulo de interface deve suportar, no mínimo, uma conexão lógica e ativa entre uma aplicação e a leitora. Em outras palavras, o módulo de interface não necessita suportar múltiplas conexões ativas com uma aplicação. Entretanto, tal funcionalidade não deve impedir o gerenciamento de sessões conforme as características definidas pelo padrão ISO/IEC 7816-4.

REQUISITO II.23: Se um módulo de interface suportar múltiplas leitoras, ele deve apresentar uma conexão lógica independente para cada leitora. Além disso, neste caso, o módulo de interface deve também suportar uma funcionalidade que possibilite determinar a associação entre uma dada leitora e sua respectiva conexão lógica.

A implementação de características relacionadas ao gerenciamento de sessões deve estar sob a responsabilidade do cartão inteligente e seu respectivo provedor de serviços (SP – *Service Provider*).

REQUISITO II.24: A documentação técnica da leitora deve descrever as características operacionais que estão implementadas no dispositivo.

B – Enumeração das funcionalidades da leitora

REQUISITO II.25: O componente "Módulo de interface" deve prover uma interface que suporte a enumeração de funcionalidades (obrigatórias e opcionais). Tal interface deve estar disponível para requisição via SP do cartão inteligente.

REQUISITO II.26: Em conformidade à codificação especificada pelo padrão PC/SC versão 1.0, parte 3, seção 3.1.2, tabela 3-1, no mínimo, uma invocação via SP deve retornar informações sobre:

- Fornecedor da leitora;
- comunicação;
- protocolos;
- gerenciamento de energia;
- características de garantia de segurança;
- características mecânicas;
- características específicas do fornecedor.

REQUISITO II.27: A documentação técnica da leitora deve descrever todas as funcionalidades disponíveis no dispositivo, mostrando de forma clara a estrutura de dados utilizada (TLV, por exemplo).

REQUISITO II.28: A documentação técnica da leitora deve descrever as versões dos seguintes componentes:

- Hardware;
- software;

- firmware.

REQUISITO II.29: A parte interessada deve prover os meios necessários para identificação pela entidade usuária externa das versões dos seguintes componentes da leitora:

- Hardware;
- software;
- firmware.

C – Eventos relacionados a um cartão inteligente

REQUISITO II.30: Considerando cartões inteligentes, dois tipos de eventos devem ser detectados pela leitora:

- Notificação de inserção do cartão inteligente;
- notificação de remoção do cartão inteligente.

O componente "módulo de interface" é a entidade responsável por notificar as camadas superiores sobre a ocorrência desses eventos.

REQUISITO II.31: A documentação técnica da leitora deve descrever todos os eventos que podem ser detectados.

D – Gerenciamento da interface com um cartão inteligente

REQUISITO II.32: O componente "módulo de interface" é responsável por tornar disponível uma interface de tal forma que seja possível requisitar o estado de um cartão inteligente.

REQUISITO II.33: Em conformidade à codificação especificada pelo padrão PC/SC versão 1.0, parte 3, seção 3.1.4, tabela 3-2, as seguintes informações devem estar disponíveis sobre o estado de um dado cartão inteligente:

- Presença de cartão inteligente;
- estado da interface com o cartão inteligente;
- cadeia de caracteres (*string*) ATR;
- tipo de cartão inteligente baseado na seqüência ATR.

REQUISITO II.34: O SCL, no mínimo, deve ser capaz de distinguir entre dois tipos de erros de comunicação:

- Cartão inteligente inoperante ou sem resposta;
- irrecuperáveis.

REQUISITO II.35: Os erros de comunicação devem ser informados ao Provedor de Serviço do cartão inteligente que está logicamente conectado.

REQUISITO II.36: A documentação técnica da leitora deve descrever as informações de estado que podem ser obtidas de um cartão inteligente, mostrando de forma clara a estrutura de dados utilizada nas respostas (TLV, por exemplo).

REQUISITO II.37: A documentação técnica da leitora deve descrever os erros de comunicação que podem ser detectados pelo dispositivo.

E – Suporte a protocolos

A Figura 4 ilustra o fluxo de informações que ocorre entre o SCL e o SP do cartão inteligente. Neste caso, o SCL oculta do nível de aplicação todos os detalhes relacionados aos protocolos.

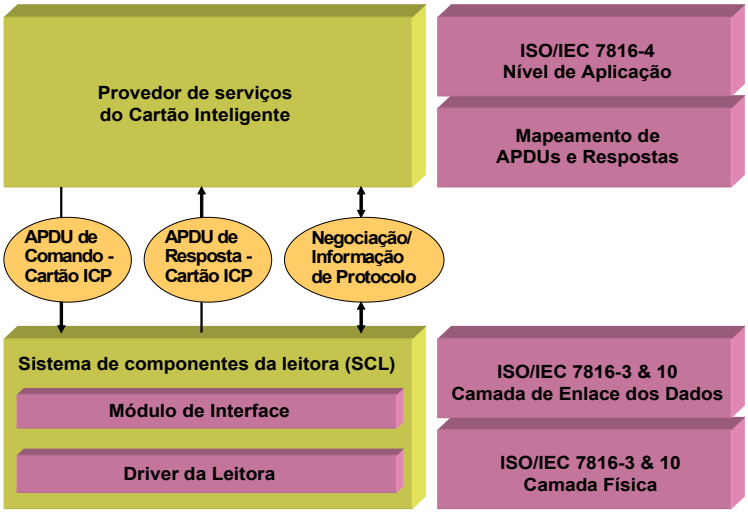

Figura 4. Mapeamento das Camadas ISO/IEC 7816 com o SCL

REQUISITO II.38: Uma leitora deve apresentar as seguintes características:

- Suportar ambos os protocolos, T=0 e T=1;
- suportar uma freqüência CLK normal (*default*) dentro do intervalo 1 a 5 Mhz.

REQUISITO II.39: Uma leitora deve esperar que uma aplicação primeiro estabeleça uma conexão lógica para depois negociar as configurações necessárias de protocolos.

Requisições de conexão lógica indicam por parte de uma aplicação o protocolo desejado e se os parâmetros de tempo devem ser otimizados ou considerados de acordo com o valor padrão (*default*).

REQUISITO II.40: Em conformidade à codificação especificada pelo padrão PC/SC versão 1.0, parte 3, seção 3.1.5, tabela 3-4, o componente "módulo de interface" deve tornar disponível uma interface que possibilite ao SP enumerar as configurações de protocolos e os parâmetros disponíveis.

2.3.4.4.2 Funcionalidades opcionais

A – Gerenciamento de energia no cartão inteligente

Uma leitora poderia permitir que um cartão inteligente inserido possa ser ativado e desativado sob o controle do SP.

Tal funcionalidade visa minimizar o consumo de energia, quando o cartão inteligente necessita estar inserido na leitora por um longo período de tempo, embora esteja sendo usado com pouca freqüência.

REQUISITO II.41: A documentação técnica da leitora deve descrever qualquer mecanismo de gerenciamento de energia que esteja implementado no dispositivo.

B – Características específicas do fornecedor

Leitoras podem implementar características que são específicas do fornecedor do dispositivo e cujas funcionalidades não foram definidas nesta especificação.

REQUISITO II.42: Características específicas do fornecedor da leitora devem ser isoladas de tal forma que não causem qualquer impacto nas funcionalidades definidas por este documento (Manual de Condutas Técnicas – Volume I).

REQUISITO II.43: Características específicas do fornecedor da leitora devem ser isoladas de tal forma que não permitam que as funcionalidades definidas por este documento (Manual de Condutas Técnicas – Volume I) sejam contornadas ou logradas.

REQUISITO II.44: A documentação técnica da leitora deve descrever todas as características que são específicas do fornecedor e estejam implementadas no dispositivo.

2.4 Requisitos de documentação

Os requisitos de documentação dizem respeito aos documentos e suas características que devem acompanhar o objeto de homologação (leitora de cartões inteligentes) na sua forma comercial.

REQUISITO IV.1: O responsável deve fornecer, no mínimo, as seguintes informações, em idioma português do Brasil, na documentação que acompanha o objeto de homologação na sua forma comercial:

- Utilização;
- instalação do driver;
- especif
- icações técnicas;
- plataformas de sistemas operacionais compatíveis;
- bibliotecas de softwares disponíveis ou compatíveis.

REQUISITO IV.2: Toda documentação relacionada a software deve informar as plataformas de sistemas operacionais suportadas e os requisitos de ambiente operacional necessários para sua operação.

REQUISITO IV.3: Todo software deve:

- Possuir ou possibilitar sua instalação em idioma português do Brasil;
- possuir tópicos de ajuda em idioma português do Brasil;
- permitir a visualização da versão do software e o nome de seu responsável.

REQUISITO IV.4: As versões dos componentes de software devem estar descritas à entidade usuária externa na documentação que acompanha o produto.

3 Parte 2

Material e documentação técnica a serem depositados para a execução do processo de homologação de leitoras de cartões inteligentes no âmbito da ICP-Brasil

3.1 Introdução

Esta parte detalha os materiais e a documentação técnica a serem depositados pela parte interessada junto ao LEA para a execução dos processos de homologação de leitoras de cartões inteligentes no âmbito da ICP-Brasil.

Os materiais e a documentação técnica referidos são classificadas em três categorias:

1. Componentes físicos: correspondem às amostras de leitoras de cartões inteligentes a serem submetidos ao processo de homologação;
2. documentação técnica: corresponde aos documentos de natureza técnica referentes aos dispositivos a serem submetidos ao processo de homologação. Devem ser depositados em formato impresso ou em formato eletrônico. No caso de formato eletrônico, devem estar armazenados, preferencialmente, em mídia tipo "leitura-somente" (*read-only*). Devem estar, obrigatoriamente, escritos nas línguas portuguesa ou inglesa;
3. componentes em softwares executáveis: correspondem aos drivers, bibliotecas de software e/ou outros softwares executáveis, solicitados por este documento, referentes aos dispositivos a serem submetidos ao processo de homologação. Devem ser depositados, obrigatoriamente, em formato eletrônico e armazenados, preferencialmente, em mídia tipo "leitura-somente" (*read-only*).

Três Níveis de Segurança de Homologação (NSH) diferentes foram estabelecidos para leitoras de cartões inteligentes:

- NSH 1: Este nível não requer depósito e análise de código fonte associado ao dispositivo em homologação;
- NSH 2: Este nível requer depósito e análise de apenas código fonte de componentes específicos associados ao dispositivo em homologação. Por exemplo, código fonte do driver da leitora;
- NSH 3: Este nível requer depósito e análise de código fonte completo associado ao dispositivo em homologação. Por exemplo, código fonte de todo software e/ou firmware da leitora de cartões inteligentes.

Para os NSHs 2 e 3, a parte interessada pode depositar o código fonte de duas maneiras diferentes:

1. Linguagem de alto nível: Código fonte deve ser depositado, por exemplo, em linguagem C, C++ ou Java. Se o código fonte estiver escrito em linguagem proprietária, o respectivo manual desta linguagem deve estar contido na documentação;
2. linguagem de baixo nível: Código fonte deve ser depositado em linguagem *assembler*, porém acompanhado do respectivo manual das instruções desta linguagem.

OBSERVAÇÃO: Para leitoras de cartões inteligentes, a parte interessada deve indicar no formulário de depósito a plataforma de sistema operacional e sua versão a ser utilizada na análise de conformidade.

3.2 Materiais e documentação técnica a serem depositados

3.2.1 Componentes físicos

Independentemente do NSH escolhido pela parte interessada, os seguintes componentes físicos devem ser depositados junto ao LEA:

- Leitora de cartões inteligentes: Amostras nas quantidades definidas por este documento para cada modelo e/ou versão de leitora de cartões inteligentes a ser submetida ao processo de homologação.

3.2.2 Documentação técnica

3.2.2.1 Nível de Segurança de Homologação 1

Os seguintes documentos técnicos devem ser depositados junto ao LEA pela parte interessada:

- Projeto de hardware: Projeto de hardware contendo o desenho esquemático do circuito eletrônico e a lista de componentes e circuitos integrados utilizados no projeto da leitora de cartões inteligentes;
- *datasheet* dos circuitos integrados: *Datasheet* dos circuitos integrados especificados no projeto de hardware da leitora de cartões inteligentes;
- Manual de comandos e intruções suportados pela leitora: Manual que descreve todas as instruções suportadas pela leitora de cartões inteligentes;

- Manual de usuário/instalação: Manual de usuário/instalação idêntico ao fornecido ao usuário;
- relação de certificados obtidos: Relação de certificação e/ou licenças obtidas para a leitora de cartões inteligentes emitidas por entidades independentes;
- documentação adicional sobre a leitora: As seguintes informações também devem estar descritas na documentação que é depositada para a análise de conformidade:
  - mecanismos de segurança:
    - algoritmos criptográficos e protocolos utilizados para troca segura de informações entre o dispositivo de entrada (PIN pad, teclado alfanumérico ou dispositivo biométrico) e o cartão inteligente;
    - mecanismos de cachê de dados de autenticação;
    - realimentação de dados de autenticação (*echo*) para uma entidade usuária externa de forma obscura durante a autenticação (por exemplo, nenhuma exibição legível de caracteres no momento da inserção de um PIN);
    - mecanismos utilizados para que dados de autenticação manipulados pela leitora estejam protegidos contra leitura não autorizada;
    - mecanismos de segurança física utilizados para previnir acesso físico não autorizado aos componentes da leitora;
    - mecanismos que mitigam ataques, como por exemplo, proteção contra vazamento de informações por emanações eletromagnéticas (*Electromagnetics Attacks – EMA*) ou por consumo de corrente (*Differential Power Analysis – DPA*).
  - Atribuição de contatos elétricos:
    - ✔ Identificação dos contatos elétricos presentes na leitora de cartões inteligentes.
  - Inserção e remoção de cartões inteligentes:
    - ✔ Mecanismos de inserção e remoção de cartões inteligentes são suportados pela leitora.
  - Propriedades elétricas:
    - ✔ Propriedade elétrica suportada que seja adicional ou não compatível aos requisitos definidos na seção 4 do padrão ISO/IEC 7816-3.

- Protocolos de transmissão de dados:
  - ✔ Protocolos de transmissão suportados em conformidade com o padrão ISO/IEC 7816-3 seções 8 e 9
- Funcionalidades do módulo de interface:
  - ✔ Descrever as características operacionais que estão implementadas no dispositivo;
  - ✔ funcionalidades disponíveis no dispositivo;
  - ✔ versões dos componentes de hardware, software e firmware;
  - ✔ eventos que podem ser detectados pela leitora;
  - ✔ informações de estado que podem ser obtidas de um cartão inteligente;
  - ✔ erros de comunicação que podem ser detectados pela leitora
  - ✔ mecanismo de gerenciamento de energia que esteja implementado na leitora;
  - ✔ características que são específicas do fornecedor e estejam implementadas na leitora.
- Documentação:
  - ✔ Plataformas de sistemas operacionais suportados e requisitos de ambiente operacional necessários para os componentes de softwares.
- Outros documentos: Projetos técnicos e suas especificações que a parte interessada julgar necessários para completar toda documentação técnica exigida por este documento.

3.2.2.2 Nível de Segurança de Homologação 2

Adicionalmente à documentação técnica solicitada no NSH 1, os seguintes itens devem ser depositados junto ao LEA pela parte interessada:

- Código fonte do driver da leitora de cartões inteligentes.

3.2.2.3 Nível de Segurança de Homologação 3

Adicionalmente à documentação técnica solicitada nos NSHs 1 e 2, os seguintes itens devem ser depositados junto ao LEA pela parte interessada:

- Código fonte do módulo de interface: Código fonte do componente “módulo de interface” da leitora de cartões inteligentes, quando aplicável;
- código fonte de software e firmware: Relação de código fonte de todo software e firmware envolvidos no funcionamento da leitora;
- código fonte de apoio: Relação de todo código fonte de apoio relacionado às interfaces de programação (API), SDK (*Software Development Kits*), ferramenta de gerenciamento e bibliotecas de software suportadas pela leitora de cartões inteligentes.

3.2.3 Componentes em softwares executáveis

Independentemente do NSH escolhido pela parte interessada, os seguintes componentes em softwares executáveis devem ser depositados junto ao LEA:

- Drivers da leitora de cartões inteligentes: Drivers da leitora de cartões inteligentes para as arquiteturas de hardware e para os sistemas operacionais suportados;
- outras bibliotecas de software e/ou programas.

3.2.4 Quantidade de materiais e documentação técnica a serem depositados para leitora de cartões inteligentes

A Tabela 2 apresenta a quantidade de materiais e documentação técnica a serem depositados pela parte interessada referente ao processo de homologação de leitoras de cartões inteligentes que se resumem em:

- Componentes físicos: amostras de cada modelo e/ou versão de leitora de cartões inteligentes;
- documentação técnica:
  - documentos impressos: devem ser entregues cópias de igual teor;
  - documentos eletrônicos: devem ser entregues cópias de igual teor e armazenadas obrigatoriamente em mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como documentos técnicos o projeto de hardware e o manual de comandos e intruções suportadas pela leitora);
- componentes em softwares executáveis: devem ser entregues cópias de igual teor e armazenadas obrigatoriamente em mídias diferentes (por

exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como componentes em softwares executáveis, o driver da leitora e outra bibliotecas de software).

Tabela 2. Quantidade de material e documentação técnica a serem depositados pela parte interessada junto ao LEA referente ao processo de homologação de leitora de cartões inteligentes

Requisito de depósito	**Material e documentação técnica a serem depositados pela parte interessada – NSH 1**	**Quantidade**
1	Leitora de cartões inteligentes	4 unidades
2	Projeto de hardware	2 cópias
3	*Datasheet* dos circuitos integrados (CI)	2 cópias
4	Manual de comandos e instruções suportadas pela leitora	2 cópias
5	Manual de usuário/instalação	2 cópias
6	Documentação adicional sobre a leitora	2 cópias
7	Relação de certificações obtidas	2 cópias
8	Outros documentos	2 cópias
Requisito de depósito	**Material e documentação técnica a serem depositados pela parte interessada – NSH 2**	
9	Código fonte do driver da leitora de cartões inteligentes	2 cópias
Requisito de depósito	**Material e documentação técnicos a serem depositados pela parte interessada – NSH 3**	
10	Código fonte exemplo de aplicação	2 cópias
11	Código fonte do módulo de interface (quando aplicável)	2 cópias
12	Código fonte de software e firmware	2 cópias
13	Código fonte de apoio	2 cópias
Requisito de depósito	**Componentes em software executável a serem depositados pela parte interessada – NSH 1, 2 e 3**	
14	Driver da leitora de cartões inteligentes	2 cópias
15	Outras bibliotecas de software e/ou programas	2 cópias

4 Referências bibliográficas

[ANSI X9.31] AMERICAN NATIONAL STANDARDS INSTITUTE. **Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)**. American Bankers Association. 1998.

[ANSI X9.62] AMERICAN NATIONAL STANDARDS INSTITUTE. **Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA).** American Bankers Association. November 2005.

[CCID 1.1] UNIVERSAL SERIAL BUS. ***Specification for Integrated Circuit(s) Cards Interface Devices.*** *Revision 1.1.* April, 2005.

[FIPS 186-2] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). **Federal Information Processing Standards Publication: *Digital Signature Standard (DSS).*** FIPS PUB 186-2. Washington. US Government Printing Office: Jan. 27, 2000.

[FIPS PUB 140-2] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). **Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules.** FIPS PUB 140-2. Washington. US Government Printing Office: May 25, 2001.

[GLOSSÁRIO ICP-BR] INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS. **Glossário ICP-Brasil.** Versão 1.2. Brasília. ICP – BR: 2007.

[IN 01/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 01/2007: Procedimentos administrativos a serem observados nos processos de homologação de sistemas e equipamentos de**

certificação digital no âmbito da ICP-Brasil. DOC-ICP-10.01. Brasília. ICP-Brasil: 2007.

[IN 02/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 02/2007: Estrutura normativa técnica e níveis de segurança de homologação a serem utilizados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil.** DOC ICP-10.02. ICP-Brasil: 2007.

[IN 03/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 03/2007: Padrões e procedimentos técnicos a serem observados nos processos de homologação de cartões inteligentes (*smart cards),* leitoras de cartões inteligentes e *tokens* criptográficos no âmbito da ICP-Brasil.** DOC-ICP-10.03. Brasília. ICP-Brasil: 2007.

[ISO/IEC 7816-2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts.** Reference Number: 7816-2. Genève, Switzerland: ISO/IEC. 1999(E).

[ISO/IEC 7816-3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols.** Reference Number: 7816-3. Genève, Switzerland: ISO/IEC. 1997(E).

[ISO/IEC 7816-3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols - AMENDMENT 1: Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V.** Reference Number: 7816-3. Genève, Switzerland, ISO/IEC: 1997/Amd. 1:2002(E).

[ISO/IEC 7816-4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange.** Reference Number: 7816-4. Genève, Switzerland, ISO/IEC : 1995(E).

[ISO/IEC 7816-5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers.** Reference Number: 7816-5. Genève, Switzerland, ISO/IEC: 1994(E).

[ISO/IEC 7816-6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements for interchange.** Reference Number: 7816-6. Genève, Switzerland, ISO/IEC: 2004(E).

[ISO/IEC 7816-7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 7: Interindustry commands for Structured Card Query Language (SCQL).** Reference Number: 7816-7. Genève, Switzerland, ISO/IEC: 1999(E).

[ISO/IEC 7816-8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 8: Commands for security operations.** Reference Number: 7816-8. Genève, Switzerland, ISO/IEC: 2004(E).

[ISO/IEC 7816-9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards –**

Integrated circuit(s) cards with contacts – Part 9: Commands for card management. Reference Number: 7816-9. Genève, Switzerland, ISO/IEC: 2004(E).

[NIST SP 800-90] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). ***Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised).*** Special Publication 800-90. Washington. US Government Printing Office: March, 2007.

[PC/SC 1.0 Part 2] PC/SC WORKGROUP. **Interoperability Specification for ICCs and Personal Computer Systems – Part 2. Interface Requirements for Compatible IC Cards and Readers.** Version 1.0. PC/SC Specification: Dec, 1997.

[PC/SC 1.0 Part 3] PC/SC WORKGROUP. **Interoperability Specification for ICCs and Personal Computer Systems – Part 3. Requirements for PC-Connected Interface Devices.** Version 1.0. PC/SC Specification: Dec, 1997.

[RSA PKCS#11] RSA LABORATORIES – PKCS#11: CRYPTOGRAPHIC TOKEN INTERFACE STANDARD. RSA Security Inc. Version 2.20. June, 2004.

[USB 2.0] UNIVERSAL SERIAL BUS REVISION 2.0 SPECIFICATION – USB-IF.

[RESOLUÇÃO 41 – ICP-BRASIL] COMITÊ GESTOR DA ICP-BRASIL. RESOLUÇÃO N° 41, DE 18 DE ABRIL DE 2006 – REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADOS NA ICP-BRASIL. ICP-BRASIL: Infra-estrutura de Chaves Públicas Brasileira. 18 de Abril de 2006.