



Infra-Estrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 1 - Volume I

Requisitos, Materiais e Documentos Técnicos para Homologação de Cartões Criptográficos (*Smart Cards*) no Âmbito da ICP-Brasil

versão 3.0

São Paulo, 22 de novembro de 2007

Sumário

CONTROLE DE VERSÃO.....	5
LISTAS DE ILUSTRAÇÕES.....	6
1INTRODUÇÃO.....	7
1.1OBJETIVO DA HOMOLOGAÇÃO.....	7
1.2DESCRIÇÃO DO PROCESSO DE HOMOLOGAÇÃO.....	7
1.3ESCOPO DESTE MANUAL.....	7
1.4ESTRUTURAÇÃO DO MCT 1 – VOLUME I.....	8
2PARTE 1.....	9
2.1INTRODUÇÃO.....	10
2.2REQUISITOS DE SEGURANÇA.....	10
2.2.1 <i>Delimitação do módulo criptográfico</i>	11
2.2.2 <i>Documentação técnica do módulo criptográfico</i>	11
2.2.3 <i>Papéis, serviços e autenticação</i>	13
2.2.3.1Papéis de acesso.....	13
2.2.3.2Serviços.....	14
2.2.3.3Identificação e autenticação de entidade usuária externa.....	14
2.2.4 <i>Modelo de estado finito</i>	18
2.2.5 <i>Segurança física</i>	19
2.2.6 <i>Ambiente operacional</i>	20
2.2.7 <i>Gerenciamento de chaves criptográficas</i>	21
2.2.7.1Geradores de números aleatórios (Random Number Generators - RNG).....	22
2.2.7.2Geração de chaves criptográficas.....	22
2.2.7.3Atribuição de chaves.....	23
2.2.7.4Importação e exportação de chaves criptográficas.....	23
2.2.7.5Armazenamento de chaves criptográficas.....	24
2.2.7.6Sobrescrita do valor de chaves criptográficas	24
2.2.8 <i>Auto-testes</i>	25
2.2.9 <i>Algoritmos criptográficos obrigatórios</i>	25
2.2.10 <i>Requisitos de PIN e PUK</i>	26
2.2.10.1PIN.....	26
2.2.10.2Bloqueio do PIN	27

2.2.10.3Troca do PIN.....	27
2.2.10.4Reinicialização do papel de acesso “Usuário”.....	27
2.2.10.5PUK.....	27
2.2.10.6Bloqueio do PUK.....	28
2.2.10.7Troca do PUK.....	28
2.2.10.8Cachê dos códigos PIN e PUK.....	28
2.2.10.9Qualidade dos códigos PIN e PUK.....	29
2.2.11Identificação de hardware, software e firmware.....	29
2.3REQUISITOS DE INTEROPERABILIDADE.....	29
2.3.1Módulo criptográfico.....	29
2.3.1.1Organização de arquivos e estrutura de dados	31
2.3.1.2Estrutura da mensagem de APDU.....	31
2.3.1.3Convenções de codificação para cabeçalhos de comandos, campos de dados e anexos (trailers) de respostas.....	32
2.3.1.4Comandos básicos de interoperabilidade.....	32
2.3.2Dimensões de contatos elétricos de cartões criptográficos ICP	34
2.3.3Número e localização de contatos elétricos em cartões criptográficos ICP.....	34
2.3.4Interface física de cartões criptográficos ICP.....	35
2.3.4.1Requisitos de interface física.....	36
2.3.4.1.1Atribuição de contatos elétricos.....	36
2.3.5Propriedades elétricas.....	37
2.3.6Transferência de dados em cartões criptográficos ICP.....	38
2.3.6.1ATR	39
2.3.6.2Protocolos de transmissão de dados.....	40
2.4REQUISITOS DE GERENCIAMENTO.....	41
2.4.1Módulos Criptográficos.....	41
2.5REQUISITOS FUNCIONAIS.....	42
2.5.1Gerenciamento de chaves criptográficas.....	43
2.5.2Exportação e importação de chaves criptográficas.....	43
2.5.3Requisitos de armazenamento.....	44
2.6REQUISITOS DE DOCUMENTAÇÃO.....	44
3PARTE 2.....	46



Infra-Estrutura de Chaves Públicas Brasileira

3.1	INTRODUÇÃO.....	47
3.2	MATERIAIS E DOCUMENTAÇÃO TÉCNICA A SEREM DEPOSITADOS.....	48
3.2.1	<i>Componentes físicos</i>	48
3.2.2	<i>Documentação técnica</i>	48
3.2.2.1	Nível de Segurança de Homologação 1.....	48
3.2.2.2	Nível de Segurança de Homologação 2.....	52
3.2.2.3	Nível de Segurança de Homologação 3.....	53
3.2.3	<i>Componentes em software executável</i>	53
3.2.4	<i>Quantidade de materiais e documentação técnica a serem depositados para o cartão criptográfico ICP</i>	53
4	REFERÊNCIAS BIBLIOGRÁFICAS.....	56

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 <i>tokens</i> 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

Figura 1. Geradores de números aleatórios.....	22
Figura 2. Arquitetura de interoperabilidade de cartões ISO 7816 e PC/SC.....	30
Figura 3. Dimensões mínimas dos contatos elétricos de cartões criptográficos ICP.....	34
Figura 4. Número e localização dos contatos elétricos em cartões criptográficos ICP.....	35
Figura 5. Identificação dos contatos elétricos para cartões criptográficos ICP segundo o padrão ISO 7816-2.....	37
Figura 6. Transferência de dados entre leitora e cartão criptográfico ICP.....	39

Lista de Tabelas

Tabela 1. Áreas de atuação do padrão FIPS 140-2.....	10
Tabela 2. Conjunto mínimo de comandos básicos de interoperabilidade para módulos criptográficos conforme padrão ISO/IEC 7816-4.....	33
Tabela 3. Identificação dos contatos para cartões criptográficos ICP.....	36
Tabela 4. Quantidade de material e documentação técnica a serem depositados pela parte interessada junto ao LEA referente ao processo de homologação de cartão criptográfico ICP 54	

1 Introdução

Este documento descreve os requisitos técnicos a serem observados no processo de homologação de cartões criptográficos (*smartcards*) ICP no âmbito da Infra-Estrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Para uma melhor compreensão do disposto neste documento, entenda-se por cartão criptográfico ICP um cartão de circuito integrado (*Integrated Circuit Card – ICC*) com capacidade de geração e armazenamento de chaves criptográficas assimétricas e processamento criptográfico assimétrico e armazenamento de certificados digitais voltados para utilização em uma Infra-Estrutura de Chaves Públicas (ICP).

1.1 Objetivo da homologação

O objetivo do processo de homologação de cartões criptográficos ICP é propiciar a interoperabilidade e operação segura do serviço criptográfico ICP oferecido por um cartão criptográfico ICP 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 um cartão criptográfico ICP 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

Cartões criptográficos ICP podem oferecer suporte a outros serviços ou subsistemas, coexistindo de forma integrada ou não com o serviço criptográfico ICP. Exemplos que podem ser citados são meios de pagamento (ex.: EMV), controle de acesso físico (ex.: PIV) e armazenamento de dados (*token* de memória).



Infra-Estrutura de Chaves Públicas Brasileira

Assim, o escopo deste manual considera o cartão criptográfico ICP, porém levando em consideração os possíveis riscos causados pela coexistência com outros serviços ou subsistemas.

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

- Componentes do módulo criptográfico:
 - Componentes eletrônicos;
 - firmware e softwares embarcados;
 - interface de comunicação;
 - módulos de software.

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

1.4 Estruturação do MCT 1 – Volume I

Este documento (MCT 1 – Volume I) está estruturado da seguinte forma:

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



2 Parte 1

Requisitos técnicos para homologação de cartões criptográficos ICP no âmbito do ICP-Brasil

2.1 Introdução

A parte 1 deste documento apresenta os requisitos técnicos que devem ser verificados no processo de homologação de cartões criptográficos ICP.

Os requisitos técnicos descritos nesta parte englobam:

- Requisitos de segurança;
- requisitos de interoperabilidade;
- requisitos de gerenciamento;
- requisitos funcionais;
- requisitos de documentação.

2.2 Requisitos de Segurança

Esta seção descreve os requisitos mínimos de segurança que devem ser atendidos pelos cartões criptográficos ICP.

Os requisitos de segurança foram elaborados com base em:

- Requisitos de segurança FIPS 140-2 nível 2 [FIPS PUB 140-2];
- requisitos de algoritmos obrigatórios;
- requisitos de PIN e PUK;
- requisitos de identificação de hardware, software e *firmware*.

O padrão FIPS 140-2 abrange onze áreas de atuação relacionadas ao projeto e implementação de um módulo criptográfico. As áreas de atuação definidas pelo padrão FIPS 140-2 são apresentadas na Tabela 1[FIPS PUB 140-2].

Tabela 1. Áreas de atuação do padrão FIPS 140-2

Seção	Áreas de atuação do padrão FIPS 140-2
1	Especificação do módulo criptográfico
2	Portas e interfaces do módulo criptográfico
3	Papéis, serviços e autenticação
4	Modelo de estado finito
5	Segurança física
6	Ambiente operacional
7	Gerenciamento de chaves criptográficas
8	Interferência e compatibilidade eletromagnética
9	Auto-testes
10	<i>Design assurance</i>
11	Mitigação de outros ataques

Das áreas de atuação definidas pelo padrão FIPS 140-2 e apresentadas na Tabela 1 apenas as 7 áreas seguintes foram consideradas na elaboração deste documento:

- Especificação do módulo criptográfico;
- papéis, serviços e autenticação;
- modelo de estado finito;
- segurança física;
- ambiente operacional;
- gerenciamento de chaves criptográficas;
- auto-testes.

Os demais requisitos de segurança (Algoritmos criptográficos obrigatórios, PIN e PUK, identificação de hardware, software e *firmware*) foram elaborados de forma a contextualizar cartões criptográficos ICP e sua aplicação na ICP-Brasil.

A menos que seja explicitamente mencionado, o termo “módulo criptográfico” é equivalente ao termo “cartão criptográfico ICP”.

2.2.1 Delimitação do módulo criptográfico

DEFINIÇÃO: Um módulo criptográfico é composto por componentes de hardware, software e *firmware* que implementam funções ou processos criptográficos delimitados por uma fronteira criptográfica.

DEFINIÇÃO: A fronteira criptográfica de um cartão criptográfico ICP é o perímetro que estabelece os limites físicos dos circuitos integrados contidos no cartão.

2.2.2 Documentação técnica do módulo criptográfico

Existem requisitos de documentação técnica, descritos a seguir, que devem ser apresentados no processo de homologação para todos os componentes de hardware, software e *firmware* relacionados à segurança da operação do módulo criptográfico.

REQUISITO I.1: A documentação técnica deve descrever os componentes de hardware, software e *firmware* do módulo criptográfico, especificando a fronteira criptográfica que delimita tais componentes.

REQUISITO I.2: A documentação técnica deve descrever a configuração física do módulo.

REQUISITO I.3: A documentação técnica deve descrever qualquer componente de hardware, software ou *firmware* que seja excluído dos requisitos de segurança apresentados neste documento e explicar a razão para tal exclusão.

REQUISITO I.4: A documentação técnica deve descrever as características elétricas, lógicas e físicas aplicáveis ao módulo.

REQUISITO I.5: A documentação técnica deve listar todas as funções de segurança e operações criptográficas que são empregadas pelo módulo, assim como especificar todos os modos de operação suportados.

REQUISITO I.6: A documentação técnica deve descrever o diagrama de blocos detalhando todos os componentes de hardware e de interconexão, incluindo:

- Microprocessadores;
- *buffers* de entrada e saída de dados;
- *buffers* com conteúdo de texto claro;
- *buffers* com conteúdo de texto cifrado;
- *buffers* de controle;
- memórias de armazenamento das chaves criptográficas;
- memórias de armazenamento dos componentes de software do módulo, tornando explícito onde foram implementados o SO (sistema operacional) e os algoritmos criptográficos;
- memória de trabalho ou operacional;
- memória de programa.

REQUISITO I.7: A documentação técnica deve descrever o projeto dos componentes de hardware, software e *firmware* do módulo criptográfico.

REQUISITO I.8: A documentação técnica deve descrever todos os dados que são relacionados à segurança, descrevendo a forma e o local de armazenamento dos dados nos componentes de hardware. Dados relacionados à segurança incluem, mas podem não estar limitados a:

- Chave criptográfica em texto claro e cifrada ;
- dado de autenticação, como por exemplo, senha e PIN;
- parâmetros críticos de segurança (PCS).

REQUISITO I.9: A documentação técnica deve descrever a política de segurança adotada pelo módulo criptográfico. A política de segurança deve descrever as regras ou procedimentos que são derivados dos requisitos definidos neste documento ,

assim como as regras ou procedimentos que foram derivados de quaisquer outros padrões ou requisitos adicionais impostos pelo fabricante.

2.2.3 Papéis, serviços e autenticação

REQUISITO I.10: O módulo criptográfico deve suportar o conceito de papel de acesso para associação com entidades usuárias externas e serviços oferecidos pelo módulo.

2.2.3.1 Papéis de acesso

REQUISITO I.11: O módulo criptográfico deve suportar, no mínimo, os seguintes papéis de acesso:

- Usuário: Realização de serviços de segurança oferecidos pelo módulo após sua iniciação, incluindo operações criptográficas, geração de chaves criptográficas, o uso do sistema de arquivos, sobrescrita do valor de chaves criptográficas (*key zeroization*), etc;
- Oficial de segurança: Realização de serviços relacionados à iniciação do sistema de arquivo do módulo, gerenciamento do módulo, reiniciação do módulo, sobrescrita do valor de chaves criptográficas (*key zeroization*) e destruição do módulo.

OBSERVAÇÃO: Uma entidade usuária externa não necessita assumir um papel de acesso para executar um serviço que não modifique, ou não substitua chaves criptográficas públicas ou que não afetem a segurança do módulo, das chaves criptográficas secretas e de PCSs, com relação à leitura, modificação, utilização ou substituição não autorizada. Exemplos de serviços que podem ser executados sem que a entidade usuária externa necessite assumir um papel de acesso, incluem:

- Informe de estado;
- auto-teste;
- leitura de certificado digital armazenado em EF (*Elementary Files*).

REQUISITO I.12: A documentação técnica deve descrever todos os papéis de acesso que são suportados pelo módulo criptográfico.

OBSERVAÇÃO: Em um determinado momento, uma entidade usuária externa pode assumir um único papel. Porém, uma mesma entidade usuária externa, em diferentes momentos, pode assumir diferentes papéis.

2.2.3.2 Serviços

DEFINIÇÃO: O termo serviço faz referência a qualquer serviço, operação ou função que possa ser realizada pelo módulo criptográfico.

DEFINIÇÃO: Uma entrada de serviço representa qualquer entrada de dado ou controle que inicie ou realize um serviço, operação ou função específica. Uma saída de serviço representa qualquer saída de dado ou estado resultante da execução de um serviço, operação ou função iniciada por uma entrada de serviço. Toda entrada de serviço deve resultar em uma saída de serviço.

REQUISITO I.13: A documentação técnica deve descrever:

- Os serviços oferecidos pelo módulo criptográfico;
- para cada serviço oferecido pelo módulo criptográfico, suas entradas de serviço, suas correspondentes saídas de serviço e os papéis de acesso autorizados nos quais o serviço pode ser realizado;
- qualquer serviço fornecido pelo módulo criptográfico para o qual uma entidade usuária externa não necessita assumir um papel autorizado. Considerando estes serviços, deve ser esclarecido que não modifiquem ou substituam chaves criptográficas públicas e que não afetem a segurança do módulo, das chaves criptográficas secretas e dos PCSs, com relação à leitura, modificação, utilização ou substituição não autorizada.

2.2.3.3 Identificação e autenticação de entidade usuária externa

Mecanismos de identificação e autenticação devem ser utilizados para identificar e autenticar uma entidade usuária externa no momento de acesso ao módulo criptográfico. Estando a entidade usuária externa devidamente identificada e autenticada é possível verificar se tal entidade está autorizada a executar um determinado serviço.

No caso do módulo criptográfico, escopo deste documento, ou seja, cartão criptográfico ICP, podem ser utilizadas duas formas de identificação e autenticação de entidade usuária externa:

- Identificação e autenticação do papel de acesso da entidade;
- identificação e autenticação da entidade.

A forma mais usual e definida no padrão ISO 7816 é a identificação e autenticação do papel da entidade, sendo ela realizada através do PIN e PUK. A entidade usuária externa deve informar ao módulo criptográfico o valor do PIN a fim de assumir o papel de usuário ou o valor do PUK para assumir o papel de oficial de segurança.

Dependendo do nível de segurança e do serviço a ser utilizado, o módulo criptográfico pode utilizar diferentes mecanismos de autenticação e controle de acesso.

DEFINIÇÃO: Mecanismos de identificação e autenticação da entidade usuária externa:

- Sem identificação e autenticação: Alguns serviços oferecidos pelo módulo criptográfico podem não requisitar identificação e autenticação da entidade usuária externa. Como exemplo é possível citar a leitura de *Elementary Files* contendo certificados digitais;
- sem autenticação: Os acessos são realizados sem autenticação;
- identificação e autenticação baseada em papel de acesso: O módulo criptográfico requisita à entidade usuária externa a seleção de um papel de acesso e sua autenticação neste papel. A seleção do papel pode ser explícita ou implícita. A entidade usuária externa pode, também, selecionar um ou mais papéis de acesso. O módulo criptográfico não necessita autenticar individualmente a identidade da entidade usuária externa. Se o módulo criptográfico permitir a uma entidade usuária externa alterar seu papel, então o módulo deve autenticar qualquer papel de acesso que não foi previamente autenticado. Por exemplo:
 - Identificação e autenticação baseada em PIN: O valor de PIN é utilizado para identificação e autenticação do papel de acesso usuário a ser assumido pela entidade usuária externa;
 - identificação e autenticação baseada em identidade: O módulo criptográfico requisita:
 - a) que a entidade usuária externa seja individualmente identificada;
 - b) que um ou mais papéis sejam, implicitamente ou explicitamente, selecionados pela entidade usuária externa (seleção de papéis);
 - c) autenticar a identidade da entidade usuária externa e autorizar a entidade usuária externa a assumir o papel selecionado.

Se o módulo criptográfico permitir a uma entidade usuária externa assumir um outro papel, então o módulo deve ou autenticar a entidade usuária externa previamente identificada ou verificar a autorização da entidade usuária externa em assumir o papel requisitado. Por exemplo:

- Identificação e autenticação baseada em nome de usuário e senha: A partir da identificação do usuário (por exemplo, um nome de usuário) é requisitada uma senha para autenticação desta identidade.

REQUISITO I.14: O módulo criptográfico deve empregar os mecanismos de identificação e autenticação baseado em papel de acesso ou baseado em identidade para controlar o acesso ao módulo criptográfico.

OBSERVAÇÃO: Um módulo criptográfico pode permitir a uma entidade usuária externa identificada e autenticada executar vários serviços associados ao papel de acesso autorizado ou pode exigir uma identificação e autenticação separada para cada serviço ou diferentes conjuntos de serviços.

REQUISITO I.15: Quando o módulo criptográfico for desligado e na seqüência ligado novamente, os resultados das identificações e autenticações prévias não devem ser mantidos. Neste caso, o módulo criptográfico sempre deve requisitar que a entidade usuária externa seja novamente identificada e autenticada.

Outras formas de identificação e autenticação podem ser utilizadas pelo módulo criptográfico, incluindo, mas não limitado a:

- Conhecimento ou posse de chave criptográfica ou equivalente;
- verificação de características pessoais, como por exemplo, biometria.

REQUISITO I.16: Dados de autenticação armazenados no interior do módulo criptográfico devem ser protegidos contra leitura, modificação, utilização e substituição não autorizada.

OBSERVAÇÃO: Se o módulo criptográfico não conter dados de autenticação necessários para autenticar a entidade usuária externa na primeira vez na qual é realizado o acesso ao módulo, então outros métodos, como por exemplo, controles no processo ou dados de autenticação padrão (“*default*”), devem ser usados para controlar o primeiro acesso ao módulo e iniciar os mecanismos de autenticação da entidade usuária externa.

REQUISITO I.17: A força ou robustez do mecanismo de autenticação deve estar em conformidade com as seguintes especificações:

- Para cada tentativa de uso do mecanismo de autenticação, a probabilidade deve ser menor do que 1 em 1.000.000, de que uma tentativa aleatória tenha sucesso, ou que uma aceitação falsa possa ocorrer (por exemplo, adivinhação de senha ou PIN, taxa de erro de aceitação falsa de um parâmetro biométrico ou alguma combinação de métodos de autenticação).

REQUISITO I.18: No contexto da CSP do cartão criptográfico ICP, a força ou robustez do mecanismo de autenticação deve estar em conformidade com as seguintes especificações:

- A realimentação de dados de autenticação (*echo*) para uma entidade usuária externa deve ser obscura durante a autenticação (por exemplo, nenhuma exibição visível de caracteres deve haver no momento da inserção de um PIN);
- não devem haver métodos alternativos oferecidos a entidade usuária externa durante uma tentativa de autenticação que enfraqueçam a força ou robustez do mecanismo de autenticação.

REQUISITO I.19: A documentação técnica deve descrever:

- Os mecanismos de autenticação suportados pelo módulo criptográfico;
- os tipos de dados de autenticação que são requisitados pelo módulo para implementar os mecanismos de autenticação suportados;
- os métodos que são utilizados para realizar o controle de acesso ao módulo criptográfico no seu primeiro acesso e, em seguida, iniciar o mecanismo de autenticação;
- a força e robustez dos mecanismos de autenticação suportados pelo módulo e pela CSP do cartão criptográfico ICP.

2.2.4 Modelo de estado finito

A operação do módulo criptográfico deve ser descrita por meio de um modelo de estado finito (ou equivalente) representado por um diagrama de transição de estados e/ou uma tabela de transição de estados.

REQUISITO I.20: O módulo criptográfico deve incluir os seguintes estados operacionais e estados de erro:

- Estados de alimentação de energia: Estados para alimentação de energia primária, secundária ou backup. Estes estados podem diferenciar em função das fontes de energia que estão sendo aplicadas ao módulo criptográfico;
- estados do oficial de segurança: Estados nos quais os serviços do oficial de segurança são executados (por exemplo, iniciação e gerenciamento de chaves criptográficas);
- estados de entrada de chave ou PCSs: Estados para a inserção de chaves criptográficas e PCSs no módulo criptográfico;
- estados de usuário: Estados nos quais entidades usuárias externas no papel de acesso usuário executam serviços de segurança, realizam operações criptográficas ou desempenham outras funções;
- estados de auto-teste: Estados nos quais o módulo criptográfico realiza auto-testes;
- estados de erro: Estados quando o módulo criptográfico encontra um erro (por exemplo, falha em um auto-teste ou tentativa de cifrar quando chaves operacionais ou PCSs foram perdidos). Estados de erro poderiam incluir:
 - a) “Erros rígidos”, os quais indicam um mal funcionamento do equipamento, podendo ser necessário executar serviços de manutenção ou reparo no módulo criptográfico;
 - b) “Erros leves e recuperáveis”, os quais requerem apenas uma nova iniciação (*resetting*) do módulo criptográfico. A recuperação a partir de estados de erro deve ser possível, exceto para os casos em que ocorram os “Erros rígidos”.

OBSERVAÇÃO: O módulo criptográfico pode, ainda, utilizar outros estados, incluindo, mas não limitado a:

- Estados de manutenção: Estados para manutenção e prestação de serviços ao módulo criptográfico, incluindo testes de manutenção lógicos e físicos. Se o módulo criptográfico contém um papel de acesso de manutenção, então um estado de manutenção deve ser incluído.

REQUISITO I.21: A documentação do módulo criptográfico deve incluir o modelo de estado finito (ou equivalente), utilizando um diagrama de transição de estados e/ou uma tabela de transição de estados que representa a operação do módulo criptográfico descrevendo:

- Todos os estados de erro e operacionais do módulo criptográfico;
- as transições correspondentes de um estado para outro;
- os eventos de entrada, incluindo inserções de dados e controles, que causam transições de um estado para outro;
- os eventos de saída, incluindo condições internas do módulo criptográfico, saídas de dados, e saídas de estado resultantes de transições de um estado para outro.

2.2.5 Segurança física

O módulo criptográfico deve empregar controles de segurança física para restringir acessos físicos não autorizados ao seu conteúdo e, também, para evidenciar a leitura, modificação, utilização ou até mesmo a substituição não autorizada de componentes do módulo.

Quanto ao tipo de circuito, o módulo criptográfico pode ser classificado em mono-CI (Mono Circuito Integrado), multi-CI (Multi Circuito Integrado):

- Mono-CI: O único circuito integrado presente no módulo criptográfico deve ser protegido por um invólucro;
- multi-CI: Os vários circuitos integrados presentes no módulo criptográfico devem ser protegidos por um invólucro.

REQUISITO I.22: Os circuitos integrados presentes em um módulo criptográfico devem ser protegidos por um invólucro. O invólucro consiste de uma cobertura com revestimento que evidencie violações. Sua finalidade é deter a observação, sondagem ou manipulação do chip sem que haja a remoção do invólucro, provendo evidências sobre tentativas de violar ou remover os componentes protegidos.

REQUISITO I.23: A documentação técnica deve descrever qual a classificação do módulo criptográfico quanto ao tipo de circuito.

REQUISITO I.24: A documentação técnica deve descrever qual a composição dos materiais empregados na fabricação do invólucro que garante a segurança física do módulo criptográfico.

REQUISITO I.25: O invólucro que evidencia violações deve ser opaco no “*spectrum*” de luz visível.

2.2.6 Ambiente operacional

O ambiente operacional de um módulo criptográfico faz referência aos componentes de software, *firmware* e hardware necessários para sua operação.

Um módulo criptográfico, quanto ao seu ambiente operacional, pode ser classificado em:

- Ambiente operacional de propósito geral: faz referência ao uso de um sistema operacional de propósito geral e comercial;
- ambiente operacional limitado: Ambiente operacional estático e não modificável, não baseado num sistema operacional de propósito geral para seu suporte;
- ambiente operacional modificável: Ambiente operacional passível de ser reconfigurado para adicionar, remover ou modificar funcionalidades. Ambientes operacionais são considerados modificáveis quando os componentes de software ou *firmware* podem ser modificados por operadores, ou então, quando operadores podem carregar e executar software ou *firmware* que não foi incluído como parte do processo de certificação do módulo.

Para módulos criptográficos do tipo cartão criptográfico ICP de ambiente operacional limitado (estático não modificável) e monoaplicação ou multiaplicação não existem requisitos de segurança associados ao ambiente operacional.

Para módulos criptográficos do tipo cartão criptográfico ICP de ambiente operacional limitado e multiaplicação existem requisitos técnicos adicionais relacionados ao seu ambiente operacional que serão tratados em outro Manual de Condutas Técnicas.

2.2.7 Gerenciamento de chaves criptográficas

O gerenciamento de chaves criptográficas abrange o ciclo de vida completo das chaves criptográficas, seus componentes e PCSs empregados pelo módulo. Abrange a geração de números aleatórios, a geração de chaves, a atribuição de chaves, a importação e exportação de chaves, o armazenamento de chaves e a sobrescrita do valor da chave com zeros.

DEFINIÇÃO: Chave criptográfica cifrada faz referência a uma chave que é cifrada utilizando um algoritmo de segurança aprovado pela família de padrões FIPS.

DEFINIÇÃO: PCS cifrado faz referência a um PCS que é cifrado utilizando um algoritmo de segurança aprovado pela família de padrões FIPS.

OBSERVAÇÃO: Chaves criptográficas e PCSs cifrados utilizando um algoritmo de segurança não aprovado pela família de padrões FIPS serão considerados em formato de texto claro.

REQUISITO I.26: Chaves simétricas, chaves assimétricas privadas e PCSs devem estar protegidas dentro do módulo contra leitura, modificação, utilização e substituição não autorizada.

REQUISITO I.27: Chaves públicas devem estar protegidas dentro do módulo contra modificação e substituição não autorizada.

REQUISITO I.28: A documentação técnica deve descrever todas as chaves criptográficas, seus componentes e PCSs empregados pelo módulo.

REQUISITO I.29: A documentação técnica deve descrever quais métodos são usados pelo módulo criptográfico para proteger chaves simétricas, chaves assimétricas privadas e PCSs contra leitura, modificação, utilização e substituição não autorizada.

REQUISITO I.30: A documentação técnica deve descrever quais métodos são usados pelo módulo criptográfico para proteger chaves públicas contra modificação e substituição não autorizada.

2.2.7.1 Geradores de números aleatórios (*Random Number Generators - RNG*)

REQUISITO I.31: Algoritmos RNG determinísticos aprovados pela família de padrões FIPS devem ser usados pelo módulo criptográfico para geração de chaves ou para gerar vetores de iniciação (IV) definidos em algoritmos criptográficos (ver Figura 1).

REQUISITO I.32: Algoritmos RNG não aprovados pela família de padrões FIPS devem ser usados somente para gerar, sementes para RNG determinísticos aprovados ou vetores de iniciação (IV) de algoritmos criptográficos (ver Figura 1).

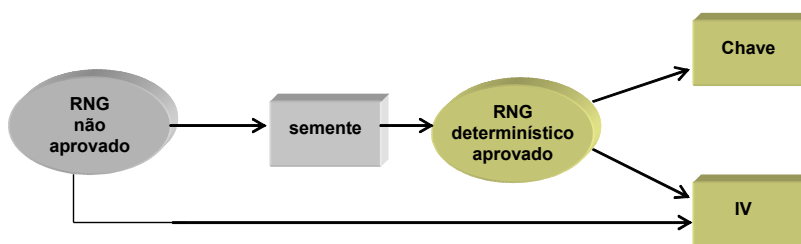


Figura 1. Geradores de números aleatórios

REQUISITO I.33: A documentação técnica deve descrever cada RNG empregado pelo módulo, seja ele aprovado ou não pelo padrão FIPS [FIPS 186-2, ANSI X9.31, ANSI X9.62-1998 e NIST SP 800-90].

2.2.7.2 Geração de chaves criptográficas

REQUISITO I.34: O módulo deve usar somente os métodos aprovados pela família de padrões FIPS para a geração de chaves criptográficas. Se um dos métodos de geração de chaves criptográficas necessitar como entrada o resultado de um RNG, então o RNG utilizado também deve ser aprovado pela família de padrões FIPS.

REQUISITO I.35: O esforço para comprometer a segurança de um método de geração de chaves criptográficas, deve ser, no mínimo, igual ao esforço para determinar o valor da chave gerada.

REQUISITO I.36: Se uma semente for inserida no módulo criptográfico para servir como entrada durante o processo de geração de chaves criptográficas, então a entrada desta semente deve atender aos requisitos especificados na seção 2.2.7.4 (“Importação e exportação de chaves criptográficas”).

REQUISITO I.37: A documentação técnica deve descrever cada um dos métodos de geração de chaves criptográficas empregados pelo módulo (aprovados ou não pela família de padrões FIPS).

2.2.7.3 Atribuição de chaves

DEFINIÇÃO: O processo ou protocolo de atribuição de chaves (*key establishment*) possibilita atribuir uma chave criptográfica simétrica compartilhada a parceiros legítimos. A atribuição de chaves pode ser realizada por um processo automático (protocolo de negociação de chaves ou protocolo de transporte de chaves), método manual ou uma combinação dos anteriores.

DEFINIÇÃO: Um método manual de atribuição de chaves é aquele no qual é utilizado um dispositivo de armazenamento para o transporte manual da chave.

DEFINIÇÃO: O processo ou protocolo de negociação de chaves (*key agreement*) possibilita atribuir uma chave criptográfica simétrica compartilhada aos parceiros legítimos em função de valores secretos escolhidos por cada um dos parceiros, de forma que nenhuma outra entidade possa determinar o valor da chave criptográfica. Exemplo de negociação de chaves é o algoritmo *Diffie-Hellman*.

DEFINIÇÃO: O processo ou protocolo de transporte de chaves (*key transport*) possibilita que uma chave criptográfica simétrica compartilhada seja transferida aos participantes legítimos da entidade geradora para parceiros. Neste método, a chave é definida por uma das entidades e repassada para as demais.

REQUISITO I.38: Se métodos de atribuição de chaves são empregados pelo módulo criptográfico, então somente os métodos de atribuição de chaves aprovados pela família de padrões FIPS devem ser usados.

REQUISITO I.39: Quando aplicável, a documentação deve descrever os métodos de atribuição de chaves empregados pelo módulo criptográfico (automático, manual ou combinação dos anteriores).

2.2.7.4 Importação e exportação de chaves criptográficas

Chaves criptográficas podem ser importadas ou exportadas de um módulo criptográfico usando um método manual ou um método automático.

REQUISITO I.40: Se o módulo criptográfico permitir a importação de chave criptográfica simétrica, chave criptográfica assimétrica privada ou PCSs, então as chaves criptográficas e PCSs devem ser cifrados utilizando algoritmos aprovados pela família de padrões FIPS.

OBSERVAÇÃO: Uma chave assimétrica pública pode ser importada ou exportada do módulo criptográfico em texto claro.

REQUISITO I.41: Não deve ser possível exportar uma chave criptográfica assimétrica privada do módulo criptográfico.

REQUISITO I.42: O módulo criptográfico deve associar a chave importada ou exportada à entidade correta a qual a chave está vinculada.

REQUISITO I.43: A documentação técnica deve descrever os métodos de importação e exportação de chaves criptográficas simétricas, chaves criptográficas assimétricas privadas e PCSs empregados pelo módulo, os algoritmos criptográficos utilizados nos métodos de importação e exportação.

2.2.7.5 Armazenamento de chaves criptográficas

DEFINIÇÃO: Chaves criptográficas devem ser armazenadas dentro do módulo criptográfico em texto claro ou de forma cifrada.

REQUISITO I.44: Chaves assimétricas privadas e chaves simétricas não devem estar acessíveis por entidades usuárias externas e não autorizadas.

REQUISITO I.45: Chaves assimétricas privadas e chaves simétricas, caso estejam armazenadas no módulo criptográfico na forma cifrada, devem utilizar algoritmos criptográficos aprovados pela família de padrões FIPS.

REQUISITO I.46: O módulo criptográfico deve associar a cada chave armazenada (simétrica ou assimétrica) à sua respectiva entidade proprietária.

REQUISITO I.47: A documentação técnica deve descrever os métodos de armazenamento de chaves criptográficas empregados pelo módulo.

2.2.7.6 Sobrescrita do valor de chaves criptográficas

REQUISITO I.48: O módulo deve prover métodos para sobrescrever os valores de chaves criptográficas e PCSs.

REQUISITO I.49: A documentação técnica deve descrever os métodos de sobrescrita dos valores de chaves criptográficas e PCSs que são empregados pelo módulo.

2.2.8 Auto-testes

REQUISITO I.50: Para verificar o funcionamento apropriado do módulo criptográfico, duas categorias de auto-testes devem ser realizadas:

- Auto-testes de energia: tais testes devem ser executados quando o módulo é energizado (ou alimentado com energia elétrica);
- auto-testes condicionais: tais testes devem ser executados quando uma operação ou função de segurança for invocada.

REQUISITO I.51: O módulo não deve realizar qualquer operação criptográfica enquanto o estado de erro provocado por falhas em um auto-teste persistir.

REQUISITO I.52: A documentação técnica do módulo criptográfico deve incluir descrições sobre:

- Os auto-testes realizados pelo módulo criptográfico dentro das categorias citadas no **REQUISITO I.50**;
- os estados de erro que o módulo criptográfico alcança quando um auto-teste falha;
- as condições e ações necessárias para retirar os estados de erro e reiniciar a operação normal do módulo criptográfico.

2.2.9 Algoritmos criptográficos obrigatórios

REQUISITO I.53: O módulo criptográfico deve suportar os seguintes sistemas criptográficos:

- Criptografia de dados:
 - DES (*Data Encryption Standard*) no modo CBC, apenas para uso legado (conforme padrão NIST FIPS PUB 46-3);
 - *Triple-DES* (3DES ou TDES) no modo CBC (conforme padrão NIST FIPS PUB 46-3);
 - RSA com tamanho mínimo de chaves de 1024 bits (conforme padrões NIST FIPS PUB 186-2 e PKCS #1 v. 2.1).
- Autenticação de entidades com criptografia de Chaves Públicas:
 - RSA com tamanho mínimo de chaves de 1024 bits (conforme padrões NIST FIPS PUB 186-2 e PKCS #1 v. 2.1).
- Resultado *Hash*:
 - SHA-1 (*Secure Hash Algorithm*) segundo padrão NIST FIPS PUB 180-2.

RECOMENDAÇÃO I.1: De forma opcional, é recomendado que o módulo criptográfico também possa suportar os seguintes sistemas criptográficos:

- Criptografia de dados:
 - AES (*Advanced Encryption Standard*) com tamanho mínimo de chaves de 128 bits (conforme padrão NIST FIPS PUB 197).
- Autenticação de entidades com criptografia de Chaves Públicas:
 - DSA (*Digital Signature Algorithm*) com tamanho mínimo de chaves de 512 bits (conforme padrão NIST FIPS PUB 186-2).
- Resultado *Hash* segundo o padrão NIST FIPS PUB 180-2:
 - SHA-224;
 - SHA-256;
 - SHA-384;
 - SHA-512.

2.2.10 Requisitos de PIN e PUK

2.2.10.1 PIN

REQUISITO I.54: No módulo criptográfico, o uso da chave assimétrica privada deve ser habilitado apenas nos casos de identificação e autenticação bem sucedida do papel de acesso Usuário, ou seja, somente após a inserção correta do PIN por parte da entidade usuária externa.

REQUISITO I.55: O PIN que habilita acesso ao papel usuário deve ser escolhido, exclusivamente, pela entidade usuária externa do módulo criptográfico.

2.2.10.2 Bloqueio do PIN

REQUISITO I.56: Por questões de segurança (contra ataques de adivinhação do PIN por meio de sucessivas tentativas), o módulo criptográfico deve bloquear o PIN do papel de acesso usuário após, no máximo, 5 tentativas mal sucedidas.

2.2.10.3 Troca do PIN

REQUISITO I.57: Quando aplicável, o módulo criptográfico deve forçar que, no primeiro acesso, o proprietário altere o PIN padrão.

REQUISITO I.58: O módulo criptográfico deve possibilitar a entidade usuária externa alterar o PIN do papel de acesso usuário, a qualquer momento, por sua própria iniciativa. Nesta situação, tal alteração deve ocorrer somente mediante uma inserção correta do PIN atual e duas inserções do novo PIN escolhido.

2.2.10.4 Reinicialização do papel de acesso “Usuário”

REQUISITO I.59: O papel de acesso “Usuário”, e conseqüentemente o valor do PIN associado, nunca deve ser reinicializado individualmente. Quando o papel de acesso “Usuário” for reinicializado, as chaves criptográficas associadas devem ser eliminadas.

REQUISITO I.60: Para possibilitar a reutilização do módulo criptográfico pelo usuário, a reinicialização do papel de acesso “usuário” e conseqüentemente o valor do PIN e chaves criptográficas, deve ser realizada mediante inserção correta do PUK pela entidade usuária externa.

2.2.10.5 PUK

DEFINIÇÃO: O PUK (PIN *Unlock Key*) é um código alfanumérico usado como chave para habilitar o desbloqueio e/ou alteração do PIN. Neste documento, o PUK será considerado como o PIN do oficial de segurança.

REQUISITO I.61: O módulo criptográfico deve permitir ao usuário, após informar corretamente o PUK, desbloquear e/ou trocar o PIN corrente.

2.2.10.6 Bloqueio do PUK

REQUISITO I.62: Por questões de segurança (contra ataques de adivinhação do PUK por meio de sucessivas tentativas), o módulo criptográfico deve bloquear o PUK após, no máximo, 5 tentativas mal sucedidas.

2.2.10.7 Troca do PUK

REQUISITO I.63: O módulo criptográfico deve possibilitar a alteração do PUK, a qualquer momento, por iniciativa da entidade usuária externa, sendo que tal alteração deve ocorrer somente mediante a inserção correta do PUK anterior. O PUK não pode ser alterado por outro modo.

2.2.10.8 Cachê dos códigos PIN e PUK

O “Provedor de Serviços” (PS) pode realizar o cachê de código PIN somente em uma mesma sessão de aplicação.

Os requisitos técnicos abordados nesta seção são contextualizados na CSP do cartão criptográfico ICP.

REQUISITO I.64: O código PUK nunca deve ser mantido em cachê no Provedor de Serviços.

REQUISITO I.65: O Provedor de Serviços pode manter em cachê o código PIN desde que garanta a eliminação do PIN no cachê nas seguintes situações:

- Sempre que o módulo criptográfico for desconectado de sua interface;
- sempre que a aplicação associada for encerrada.

REQUISITO I.66: A eliminação do código PIN presente no cachê deve ser realizada com sobrescrita de seu valor.

RECOMENDAÇÃO I.2: Apesar de permitida, a funcionalidade de cachê deve ser evitada sempre que possível. Quando utilizada, é recomendada a implementação de controles adicionais, como por exemplo:

- Tempo de Vida (*Time To Live* - TTL): tempo de duração máxima do PIN no cachê;
- confirmação do uso da chave pelo usuário: o usuário deve ser notificado antes da utilização da chave privada, devendo o usuário ter a opção de concordar ou não (confirmar) com o uso da chave privada.

2.2.10.9 Qualidade dos códigos PIN e PUK

Os requisitos técnicos abordados nesta seção são contextualizados na CSP do cartão criptográfico ICP.

REQUISITO I.67: O Provedor de Serviços deve aplicar controles de qualidade no momento da definição dos códigos PIN e PUK pela entidade usuária externa. Deve implementar os seguintes controles:

- Tamanho mínimo de 4 a 8 caracteres;
- sensibilidade a letras maiúsculas e minúsculas do alfabeto português (*Case Sensitive*).

2.2.11 Identificação de hardware, software e firmware

REQUISITO I.68: O cartão criptográfico ICP deve possuir elementos que permitam a identificação das versões e revisões dos seguintes componentes do módulo criptográfico:

- Hardware;
- software;
- firmware.

REQUISITO I.69: A documentação técnica do módulo criptográfico entregue para fins de homologação deve descrever as versões dos seguintes componentes:

- Hardware;
- software;
- firmware.

2.3 Requisitos de interoperabilidade

REQUISITO II.1: Cartões criptográficos ICP, 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 Módulo criptográfico

O objetivo desta seção é detalhar o conjunto de requisitos técnicos necessários para propiciar a interoperabilidade de módulos criptográficos conectados a um computador.

A Figura 2 ilustra a arquitetura de interoperabilidade de cartões ISO 7816 e PC/SC, por meio da qual aplicações podem invocar operações (criptográficas ou não) em módulos criptográficos, usando componentes do tipo SP (*Service Providers*). O componente Gerente de Recursos (*Resource Manager*) é responsável por controlar o acesso aos recursos.

Além disso, a Figura 2 também ilustra um mapeamento entre a arquitetura de interoperabilidade de cartões ISO 7816 e PC/SC e o conjunto de padrões ISO/IEC da família 7816.

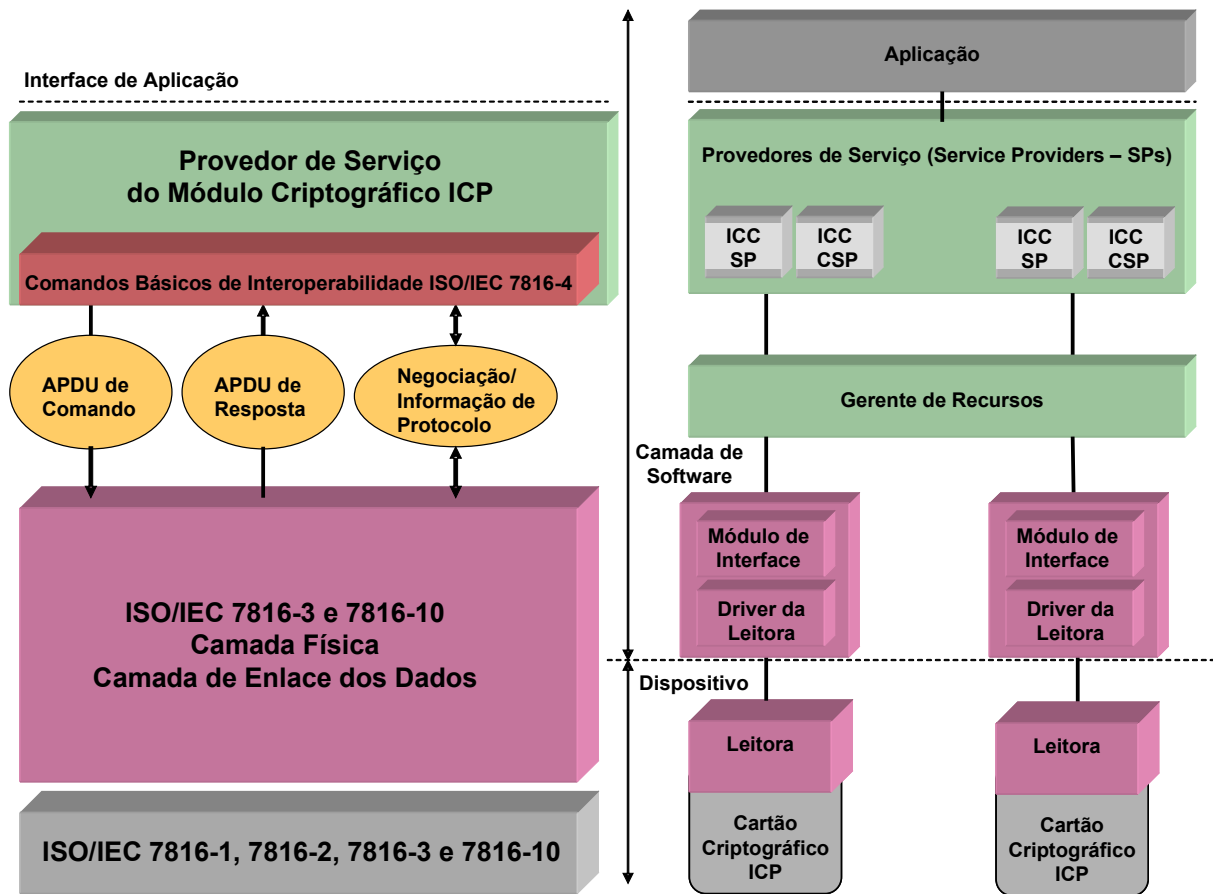


Figura 2. Arquitetura de interoperabilidade de cartões ISO 7816 e PC/SC

Portanto, conforme indicado na Figura 2, o módulo criptográfico limita seu escopo em analisar um conjunto de comandos básicos de interoperabilidade definidos pelo padrão ISO/IEC 7816-4. A análise de tais comandos, como requisito inicial de interoperabilidade, propiciará ainda a verificação de conformidade aos seguintes aspectos do padrão ISO/IEC 7816-4:

- Conteúdo dos comandos e respostas (*Application Protocol Data Unit - APDU*) transmitidas ao módulo criptográfico e vice-versa;
- estrutura dos arquivos e dados usados no processamento dos comandos básicos de interoperabilidade;
- métodos de acesso aos arquivos e dados no módulo criptográfico.

Este documento não restringe a verificação dos comandos básicos de interoperabilidade em relação à plataforma e versão de sistema operacional, ou seja, os testes de conformidade com os comandos básicos de interoperabilidade



Infra-Estrutura de Chaves Públicas Brasileira

poderão ser realizados em diferentes plataformas e versões de sistemas operacionais atualmente disponíveis (tais como, Microsoft Windows, Linux e UNIX).

2.3.1.1 Organização de arquivos e estrutura de dados

REQUISITO II.2: Um módulo criptográfico deve seguir as estruturas de dados de organização de arquivos conforme os requisitos e convenções definidas na seção 5.1 do padrão ISO/IEC 7816-4.

REQUISITO II.3: A documentação técnica deve descrever a organização de arquivos e estrutura de dados utilizada pelo módulo criptográfico.

2.3.1.2 Estrutura da mensagem de APDU

Uma aplicação necessita enviar um comando para ser processado pelo módulo criptográfico, o qual, por sua vez, retorna a respectiva resposta. Essa correspondência entre um comando emitido e sua respectiva resposta é denominada de “par comando-resposta”.

Uma APDU (*application protocol data unit*) contém um comando ou uma resposta trocada com o módulo criptográfico.

Uma APDU de comando consiste de duas partes: um cabeçalho obrigatório de 4 bytes e um corpo de tamanho variável. Da mesma forma, uma APDU de resposta consiste de duas partes: um corpo de tamanho variável e um anexo obrigatório (*trailer*) de 2 bytes.

REQUISITO II.4: Um módulo criptográfico deve seguir uma estrutura de APDU (comando e resposta) conforme os requisitos e convenções definidas na seção 5.3 do padrão ISO/IEC 7816-4.

REQUISITO II.5: A documentação técnica deve descrever a estrutura da mensagem APDU.

2.3.1.3 Convenções de codificação para cabeçalhos de comandos, campos de dados e anexos (*trailers*) de respostas

REQUISITO II.6: Considerando os campos de dados das APDUs, os cabeçalhos dos comandos e os anexos das respectivas respostas, um módulo criptográfico deve ser compatível com as convenções de codificação definidas na seção 5.4 do padrão ISO/IEC 7816-4.

2.3.1.4 Comandos básicos de interoperabilidade

De acordo com o padrão ISO/IEC 7816-4, cartões criptográficos ICP não são obrigados a suportar todos os comandos básicos definidos e nem todas as opções associadas a um dado comando.

Entretanto, com o intuito de buscar a interoperabilidade entre provedores de serviço, leitoras, módulos criptográficos e aplicações, este documento reconhece a iniciativa do padrão ISO/IEC 7816-4, e define a obrigatoriedade do atendimento a um conjunto mínimo de comandos básicos.

REQUISITO II.7: Um módulo criptográfico deve suportar, no mínimo, os comandos básicos de interoperabilidade definidos pelo padrão ISO/IEC 7816-4 conforme mostra a Tabela 2.

REQUISITO II.8: Caso um ou mais comandos descritos na Tabela 2 não sejam suportados pelo módulo criptográfico, a documentação técnica deve justificar a ausência.

Tabela 2. Conjunto mínimo de comandos básicos de interoperabilidade para módulos criptográficos conforme padrão ISO/IEC 7816-4

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 (<i>offset</i>) 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 aos objetos de dados.	6.9
PUT DATA	Utilizado para armazenar ou escrever 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 uma entidade externa perante um módulo criptográfico.	6.14
GET CHALLENGE	Requer do módulo criptográfico um número randômico (desafio – “ <i>challenge</i> ”) para ser usado posteriormente para fins de autenticação.	6.15

REQUISITO II.9: A parte interessada deve prover os meios necessários em termos de informações e bibliotecas de software para que comandos básicos de

interoperabilidade ISO/IEC 7816-4 suportados possam ser verificados no módulo criptográfico.

REQUISITO II.10: A documentação técnica deve descrever todos os comandos ISO/IEC 7816-4 e comandos proprietários suportados pelo módulo criptográfico.

2.3.2 Dimensões de contatos elétricos de cartões criptográficos ICP

REQUISITO II.11: Um cartão criptográfico ICP deve atender aos requisitos de dimensões de contatos elétricos definidos na seção 3 do padrão ISO/IEC 7816-2. A Figura 3 demonstra as dimensões mínimas para os contatos elétricos em cartões criptográficos ICP de acordo com o padrão ISO/IEC 7816-2 seção 3.

2.3.3 Número e localização de contatos elétricos em cartões criptográficos ICP

REQUISITO II.12: Um cartão criptográfico ICP deve atender aos requisitos de número e localização de contatos elétricos definidos na seção 4 do padrão ISO/IEC 7816-2. A Figura 4 demonstra o número e a localização dos contatos elétricos em cartões criptográficos ICP de acordo com o padrão ISO/IEC 7816-2 seção 4.

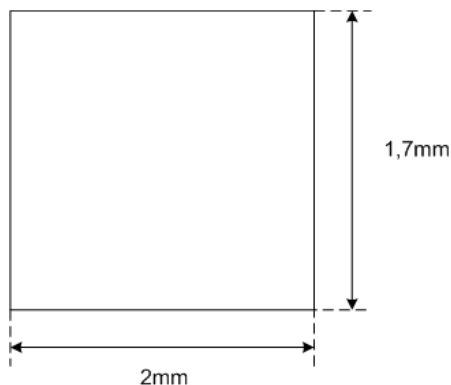


Figura 3. Dimensões mínimas dos contatos elétricos de cartões criptográficos ICP

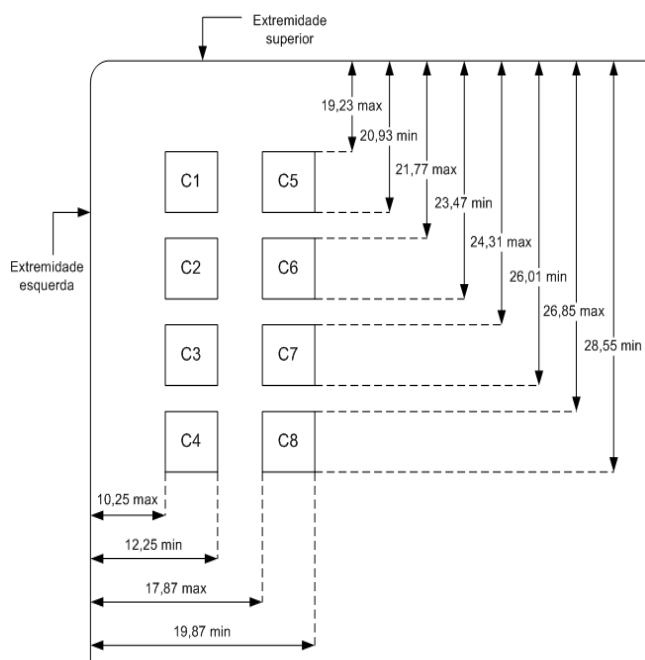


Figura 4. Número e localização dos contatos elétricos em cartões criptográficos ICP

2.3.4 Interface física de cartões criptográficos ICP

Esta seção determina os requisitos de interoperabilidade e compatibilidade que devem ser atendidos por cartões criptográficos ICP em sua interface física. 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.*

2.3.4.1 Requisitos de interface física

2.3.4.1.1 Atribuição de contatos elétricos

REQUISITO II.13: Os contatos elétricos localizados em um cartão criptográfico ICP devem ser compatíveis com os requisitos definidos na seção 5 do padrão ISO/IEC 7816-2 e identificados conforme mostra a Tabela 3.

Tabela 3. Identificação dos contatos para cartões criptográficos ICP

Identificação do contato	Descrição
C1	Voltagem de alimentação (<i>supply voltage – Vcc</i>)
C2	Sinal “reset” (RST)
C3	Sinal “clock” (CLK)
C4	Reservado para uso futuro em outras partes do ISO/IEC 7816 (não usado atualmente) - RFU (<i>reserved for future use</i>)
C5	terra – “ground” (GND)
C6	Identificado pelo padrão ISO/IEC 7816-2 como “Voltagem de programação” (<i>variable supply voltage - VPP</i>) – Geralmente não mais usado
C7	Entrada/saída de dados (<i>Data input/output – I/O</i>)
C8	Reservado para uso futuro em outras partes do ISO/IEC 7816 (não usado atualmente) - RFU (<i>reserved for future use</i>)

Portanto, cartões criptográficos ICP devem possuir até 8 áreas de contato, constituindo a interface física/elétrica entre uma leitora e um cartão criptográfico ICP.

Os contatos C4 e C8 são reservados para uso futuro e não necessitam estar operacionais.

REQUISITO II.14: Contatos não utilizados, como por exemplo, os contatos C4 e C8, caso estejam presentes no cartão criptográfico ICP, devem ser isolados, do ponto de vista elétrico (não condutíveis), do circuito integrado e de quaisquer outros contatos inseridos no cartão criptográfico ICP.

REQUISITO II.15: Se o contato C6 não for necessário para uso (contato C6 inoperante) e estiver presente no cartão criptográfico ICP, deve ser isolado, do ponto de vista elétrico (não condutível), do circuito integrado e de quaisquer outros contatos inseridos no cartão criptográfico ICP e leitora.

O contato C6 foi previamente reservado para a aplicação de uma voltagem externa na memória EEPROM, voltagem esta necessária para programar e apagar a memória. Atualmente, o contato C6 não necessita mais ser usado, pois a voltagem necessária é gerada diretamente no circuito integrado.

REQUISITO II.16: Os contatos elétricos de cartões criptográficos ICP devem seguir as disposições definidas na seção 4 da ISO 7816-2, conforme apresentado na Figura 5.

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

Figura 5. Identificação dos contatos elétricos para cartões criptográficos ICP segundo o padrão ISO 7816-2

REQUISITO II.17: A documentação técnica deve descrever a identificação dos contatos elétricos que são utilizados pelos cartões criptográficos ICP.

REQUISITO II.18: A documentação técnica deve descrever se o contato elétrico C6 é ou não necessário no cartão criptográfico ICP e, caso seja necessário, justificar o seu uso.

2.3.5 Propriedades elétricas

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

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

Além disso, existem outros requisitos de conformidade relacionados às propriedades elétricas dos cartões criptográficos ICP:

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

REQUISITO II.19: Um cartão criptográfico ICP deve atender aos requisitos de propriedades elétricas definidos na seção 4 do padrão ISO/IEC 7816-3 .

Especificamente para um cartão criptográfico ICP, para fins de interoperabilidade, ambas as classes de operação A e B devem ser suportadas.

REQUISITO II.20: A documentação do cartão criptográfico ICP deve descrever qualquer propriedade elétrica suportada que seja adicional ou não compatível aos requisitos definidos na seção 4 do padrão ISO/IEC 7816-3.

2.3.6 Transferência de dados em cartões criptográficos ICP

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

Depois que um cartão criptográfico ICP for inserido em uma leitora, seus contatos elétricos são mecanicamente conectados aos da leitora. Portanto, a leitora não deve ativar o cartão criptográfico ICP até que esteja mecanicamente conectado aos contatos da leitora.

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

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

REQUISITO II.21: O cartão criptográfico ICP deve atender aos requisitos de ativação dos circuitos elétricos por *cold reset* definidos na seção 5.3.2 do padrão ISO/IEC 7816-3.

REQUISITO II.22: O cartão criptográfico ICP deve atender aos requisitos de ativação dos circuitos elétricos por *warm reset* definidos na seção 5.3.3 do padrão ISO/IEC 7816-3.

REQUISITO II.23: O cartão criptográfico ICP deve atender aos requisitos de desativação dos circuitos elétricos (*deactivation*) definidos na seção 5.4 do padrão ISO/IEC 7816-3.

2.3.6.1 ATR

DEFINIÇÃO: ATR (*Answer To Reset*) é o valor da seqüência de bytes enviado pelo cartão criptográfico ICP à leitora como resposta ao estímulo de reinício (*reset*). Neste caso, cada byte é transportado em um caractere assíncrono.

Portanto, conforme mostra a Figura 6 cada estímulo de reinício (*reset*) bem sucedido deve resultar em uma resposta ATR por parte do cartão criptográfico ICP. 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.

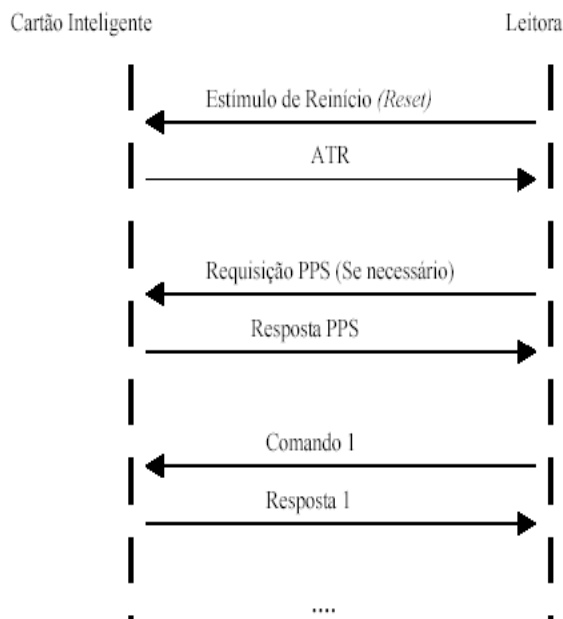


Figura 6. Transferência de dados entre leitora e cartão criptográfico ICP

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

- 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.24: Um cartão criptográfico ICP deve atender aos requisitos de ATR e PPS de acordo com o padrão ISO/IEC 7816-3 (seções 6 e 7).

2.3.6.2 Protocolos de transmissão de dados

A comunicação com um cartão criptográfico ICP pode ser implementada de diversas maneiras por meio de protocolos de transmissão de dados, envolvendo o envio de comandos, as respectivas respostas e aos 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 (*smart cards*), a saber:

- T=0: faz referência à transmissão assíncrona do tipo “*half-duplex*” orientada aos caracteres;
- T=1: faz referência à transmissão assíncrona do tipo “*half-duplex*” orientada aos 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 aos 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.25: Um cartão criptográfico ICP deve atender aos requisitos de protocolo de transmissão T=0 ou T=1 definidos pelo padrão ISO/IEC 7816-3 seções 8 e 9 respectivamente.

2.4 Requisitos de Gerenciamento

REQUISITO III.1: O módulo criptográfico deve atender aos requisitos de gerenciamento ora estabelecidos, conforme descrito nos itens a seguir.

2.4.1 Módulos Criptográficos

Os requisitos de gerenciamento fazem referência às funcionalidades que devem estar disponíveis ao proprietário do módulo criptográfico, permitindo executar operações de controle.

REQUISITO III.2: Funcionalidades de gerenciamento do módulo criptográfico devem estar disponíveis ao proprietário por meio de uma ferramenta específica ou utilitário. Tal utilitário deve ser provido pelo fornecedor do módulo criptográfico contendo, no mínimo, mas não limitado aos seguintes aspectos:

- Permitir a exportação de certificados digitais armazenados no módulo criptográfico;
- permitir a importação de certificados digitais para a área de armazenamento do módulo criptográfico;
- permitir a visualização de certificados digitais armazenados no módulo criptográfico;
- para cada certificado digital armazenado no módulo criptográfico, permitir que todos os campos contemplados pela ICP-Brasil sejam visualizados;

- permitir ao proprietário apagar chaves criptográficas e outros dados contidos no módulo criptográfico, segundo os procedimentos adequados de autenticação, caso seja necessário;
- permitir a troca do PIN por meio de confirmação e verificação, tanto do PIN atual, como por meio de duas inserções do novo PIN escolhido;
- permitir a eliminação do PIN somente mediante alerta e posterior confirmação do proprietário, conscientizando sobre o apagamento dos dados criptográficos associados;
- permitir a reutilização de módulos criptográficos.

2.5 Requisitos funcionais

Os requisitos funcionais dizem respeito à avaliação de funções relacionadas à arquitetura do módulo criptográfico que podem ser invocadas por aplicações de usuários por meio de uma interface de alto nível denominada de API (*Application Programming Interface*).

REQUISITO IV.1: O módulo criptográfico deve atender aos requisitos funcionais ora estabelecidos, conforme descrito nos itens a seguir. No escopo deste documento, pelo menos uma das seguintes API serão consideradas para análise dos requisitos funcionais:

- Microsoft CryptoAPI;
- PKCS#11;
- JCE.

REQUISITO IV.2: No mínimo, os requisitos funcionais devem estar disponíveis por invocação, via API, em uma das seguintes plataformas de sistemas operacionais:

- Linux kernel 2.4 ou versões superiores;
- Microsoft Windows 2000 / XP ou versões superiores.

2.5.1 Gerenciamento de chaves criptográficas

REQUISITO IV.3: Os seguintes requisitos funcionais de gerenciamento de chaves criptográficas devem estar disponíveis por invocação via API do sistema operacional:

- Gerar chave criptográfica assimétrica de forma randômica no módulo criptográfico;
- destruir chave criptográfica assimétrica com sobrescrita de valores;
- recuperar parâmetros sobre uma determinada chave criptográfica assimétrica, tais como:
 - algoritmo;
 - expoente público (RSA);
 - módulo (RSA);
 - tamanho da chave;
 - permissões.

2.5.2 Exportação e importação de chaves criptográficas

REQUISITO IV.4: Os seguintes requisitos funcionais de exportação e importação devem estar disponíveis por invocação via API do sistema operacional:

- Exportar chave criptográfica assimétrica pública do módulo criptográfico;
- exportar certificado digital do módulo criptográfico;
- exportar cadeia de certificação do módulo criptográfico;
- importar/exportar cadeia de certificação em/de módulo criptográfico;
- importar certificado digital para o módulo criptográfico segundo padrão X.509 versão 3;
- importar cadeia de certificação para o módulo criptográfico;
- permitir gravação no módulo criptográfico de certificados digitais compatíveis às normas ICP-Brasil e que usam a recomendação ITU-T X.509 versão 3 (conforme perfil estabelecido na RFC 2459).

2.5.3 Requisitos de armazenamento

REQUISITO IV.5: O módulo criptográfico deve possuir capacidade de armazenamento para certificados digitais de, no mínimo, 16 Kbytes.

2.6 Requisitos de documentação

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

REQUISITO V.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 dos CSPs;
- instalação e uso da ferramenta de gerenciamento;
- especificações técnicas;
- plataformas de sistemas operacionais compatíveis;
- guia de desenvolvimento;
- bibliotecas de software disponíveis.

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

REQUISITO V.3: Todo software deve:

- Possuir ou possibilitar a configuração da sua interface gráfica 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 V.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 cartões criptográficos 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 cartões criptográficos ICP (*Smart Cards*) no âmbito da ICP-Brasil.

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

1. Componentes físicos: correspondem às amostras de cartões criptográficos ICP 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 CSPs, drivers, bibliotecas de software, ferramentas de gerenciamento de dispositivo 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 cartões criptográficos ICP:

- 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 algoritmo gerador de números pseudo aleatórios;
- 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 do módulo criptográfico.

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 cartões criptográficos ICP, 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:

- Cartão criptográfico ICP: Amostras nas quantidades definidas por este documento para cada modelo e/ou versão de cartão criptográfico ICP a ser submetido 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:

- PIN e PUK padrão: Caso os valores de PIN e PUK padrão já tenham sido definidos previamente pela parte interessada, estes valores devem ser informados para cada cartão criptográfico ICP entregue para a execução do processo de análise de conformidade. Caso os valores do PIN e PUK padrão não tenham sido pré-estabelecidos, a parte interessada deve informar os procedimentos a serem adotados para definir estes valores;

- Política de segurança: Política de segurança utilizada no objeto de homologação;
- Documentação que acompanha o produto: As seguintes informações devem estar descritas na documentação que acompanha o objeto de homologação na sua forma comercial (produto):
 - ✓ Utilização do cartão criptográfico ICP;
 - ✓ instalação dos CSPs;
 - ✓ instalação e uso da ferramenta de gerenciamento;
 - ✓ especificações técnicas;
 - ✓ plataformas de sistemas operacionais compatíveis;
 - ✓ guia de desenvolvimento;
 - ✓ bibliotecas de software disponíveis;
 - ✓ plataformas de sistemas operacionais suportadas pelos softwares que acompanham o produto e requisitos de ambiente operacional necessários para operação.
- Manual de comandos APDU suportados: Manual contendo a descrição de todos os comandos APDU suportados pelo cartão inteligente, apresentando sequências de comandos APDU para executar exemplos de operações;
- Relação de certificados obtidos: Relação de certificação e/ou licenças obtidas para o módulo criptográfico emitidas por entidades independentes;
- Documentação adicional sobre o módulo criptográfico: As seguintes informações também devem estar descritas na documentação que é depositada para a análise de conformidade:
 - Módulo criptográfico:
 - ✓ Componentes de hardware, software e *firmware* do módulo criptográfico, incluindo suas respectivas versões;
 - ✓ configuração física do módulo;
 - ✓ qualquer componente de hardware, software ou *firmware* que seja excluído dos requisitos de segurança;
 - ✓ características elétricas, lógicas e físicas aplicáveis ao módulo;
 - ✓ funções de segurança e operações criptográficas que são empregadas pelo módulo, assim como todos os modos de operação suportados;

Infra-Estrutura de Chaves Públicas Brasileira

- ✓ diagrama de blocos detalhando todos os componentes de hardware e de interconexão, incluindo:
 - Microprocessadores;
 - *buffers* de entrada e saída de dados;
 - *buffers* com conteúdo de texto claro;
 - *buffers* com conteúdo de texto cifrado;
 - *buffers* de controle;
 - memórias de armazenamento das chaves criptográficas;
 - memórias de armazenamento dos componentes de software do módulo, tornando explícito onde foram implementados o SO (Sistema Operacional) e os algoritmos criptográficos;
 - memória de trabalho ou operacional;
 - memória de programa.
- ✓ projeto dos componentes de hardware, software e *firmware* do módulo criptográfico;
- ✓ todos os dados que são relacionados à segurança, descrevendo a forma e o local de armazenamento dos dados nos componentes de hardware. Dados relacionados à segurança incluem, mas podem não estar limitados a:
 - Chave criptográfica em texto claro e cifrada ;
 - dado de autenticação, como por exemplo, senha e PIN;
 - parâmetros crítico de segurança (PCS).
- ✓ política de segurança adotada pelo módulo criptográfico;
- ✓ papéis de acesso que são suportados pelo módulo criptográfico;
- Serviços:
 - ✓ Serviços oferecidos pelo módulo criptográfico e para cada serviço suas entradas de serviço, suas correspondentes saídas de serviço e os papéis de acesso autorizados no qual o serviço pode ser realizado;
 - ✓ demonstração de que para cada serviço oferecido pelo módulo, nos quais não é necessária a autenticação, a segurança do módulo criptográfico não é afetada.
- Identificação e autenticação de entidade usuária externa:
 - ✓ Mecanismos de autenticação suportados pelo módulo criptográfico;

Infra-Estrutura de Chaves Públicas Brasileira

- ✓ tipos de dados de autenticação que são requisitados pelo módulo para implementar os mecanismos de autenticação suportados;
- ✓ métodos que são utilizados para realizar o controle de acesso ao módulo criptográfico no seu primeiro acesso e, em seguida, iniciar o mecanismo de autenticação;
- ✓ força e robustez dos mecanismos de autenticação suportados pelo módulo e pela CSP do cartão criptográfico ICP.
- Modelo de estado finito:
 - ✓ Modelo de estado finito (ou equivalente), utilizando um diagrama de transição de estados e/ou uma tabela de transição de estados que representa a operação do módulo criptográfico descrevendo:
 - Todos os estados de erro e operacionais do módulo criptográfico;
 - as transições correspondentes de um estado para outro;
 - os eventos de entrada, incluindo inserções de dados e controles, que causam transições de um estado para outro;
 - os eventos de saída, incluindo condições internas do módulo criptográfico, saídas de dados, e saídas de estado resultantes de transições de um estado para outro.
- Segurança física:
 - ✓ Classificação do módulo criptográfico quanto ao tipo de circuito;
 - ✓ composição dos materiais empregados na fabricação do invólucro que garante a segurança física do módulo criptográfico.
- Gerenciamento de chaves criptográficas:
 - ✓ Chaves criptográficas, seus componentes e PCSs empregados pelo módulo;
 - ✓ métodos usados pelo módulo criptográfico para proteger chaves simétricas, chaves assimétricas privadas e PCSs contra leitura, modificação, utilização e substituição não autorizada;
 - ✓ métodos usados pelo módulo criptográfico para proteger chaves públicas contra modificação e substituição não autorizada.
- Geradores de números aleatórios (*Random Number Generators* – RNG):
 - ✓ Cada RNG empregado pelo módulo, seja ele aprovado ou não pelo padrão FIPS.

- Geração de chaves criptográficas:
 - ✓ Cada método de geração de chaves criptográficas empregado pelo módulo (aprovados ou não pela família de padrões FIPS).
- Importação e exportação de chaves criptográficas:
 - ✓ Métodos de importação e exportação de chaves criptográficas simétricas, chaves criptográficas assimétricas privadas e PCSs empregados pelo módulo, e algoritmos criptográficos utilizados nos métodos de importação e exportação.
- Armazenamento de chaves criptográficas:
 - ✓ Métodos de armazenamento de chaves criptográficas empregados pelo módulo.
- Sobrescrita do valor de chaves criptográficas:
 - ✓ Métodos de sobrescrita dos valores de chaves criptográficas e PCSs que são empregados pelo módulo.
- Auto-testes:
 - ✓ Auto-testes realizados pelo módulo criptográfico dentro das categorias: Auto-testes de energia e Auto-testes condicionais;
 - ✓ estados de erro que o módulo criptográfico alcança quando um auto-teste falha;
 - ✓ condições e ações necessárias para retirar os estados de erro e reiniciar a operação normal do módulo criptográfico.
- Outros documentos: Projetos e documentos técnicos que a parte interessada julgar necessários para complementar toda documentação técnica exigida.

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 componente PRNG (*Pseudo Random Number Generator*);
- código fonte do componente de geração de chaves;
- código fonte do componente de atribuição de chaves;
- código fonte do componente de sobrescrita de chaves;
- código fonte do componente de armazenamento de chaves;

- código fonte do componente de importação/exportação de chaves e sementes.

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 embarcado: Relação de todo código fonte de software e/ou firmware embarcados no cartão inteligente. Caso utilize tecnologia *Java Card* e possua *applets* de funções criptográficas, fornecer o código fonte desses *applets*;
- Código fonte de apoio: Relação de todo código fonte de apoio relacionado às interfaces de programação (API), SDK (*Software Development Kits*), SP (*Service Providers*), CSP, ferramenta de gerenciamento e bibliotecas de software suportadas pelo módulo criptográfico.

3.2.3 Componentes em software executável

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

- Provedor(es) de serviço criptográfico: Provedor(es) de serviço criptográfico, para as arquiteturas de hardware e para os sistemas operacionais suportados;
- ferramenta de gerenciamento do módulo criptográfico;
- outras bibliotecas de software e/ou programas.

3.2.4 Quantidade de materiais e documentação técnica a serem depositados para o cartão criptográfico ICP

A Tabela 4 apresenta a quantidade de materiais e documentação técnica a serem depositados pela parte interessada referente ao processo de homologação de cartões criptográficos ICP que se resumem em:

- Componentes físicos: amostras de cada modelo e/ou versão de cartão criptográfico ICP;
- documentação técnica:



Infra-Estrutura de Chaves Públicas Brasileira

- 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 manual de comandos APDU, a política de segurança e código fonte);
- 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, a ferramenta de gerenciamento do módulo criptográfico e o CSP do módulo criptográfico).

Tabela 4. Quantidade de material e documentação técnica a serem depositados pela parte interessada junto ao LEA referente ao processo de homologação de cartão criptográfico ICP

Requisito de depósito	Material e documentos técnicos a serem depositados pela parte interessada – NSH 1	Quantidade
1	Cartão criptográfico ICP de produção	7 unidades
2	Cartão criptográfico ICP de teste	3 unidades
3	PIN e PUK padrão	
4	Política de segurança	2 cópias
5	Documentação que acompanha o produto	2 cópias
6	Manual de comandos APDU suportados	2 cópias
7	Relação de certificados obtidos	2 cópias
8	Documentação adicional sobre o módulo criptográfico	2 cópias
9	Outros documentos	2 cópias
Requisito de depósito	Material e documentos técnicos a serem depositados pela parte interessada – NSH 2	Quantidade
10	Código fonte do componente PRNG (<i>Pseudo Random Number Generator</i>);	2 cópias
11	Código fonte do componente de geração de chaves;	2 cópias
12	Código fonte do componente de atribuição de chaves;	2 cópias
13	Código fonte do componente de sobrescrita de chaves;	2 cópias
14	Código fonte do componente de armazenamento de chaves;	2 cópias
15	Código fonte do componente de importação/exportação de chaves e sementes;	2 cópias
Requisito de depósito	Material e documentos técnicos a serem depositados pela parte interessada – NSH 3	Quantidade
16	Código fonte embarcado	2 cópias
17	Código fonte de apoio	2 cópias
Requisito de depósito	Componentes em software executável a serem depositados pela parte interessada – NSH 1, 2 e 3	Quantidade
18	Provedor(es) de serviço criptográfico	2 cópias
19	Ferramenta de gerenciamento do módulo criptográfico	2 cópias
20	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**



Infra-Estrutura de Chaves Públicas Brasileira

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.