Infraestrutura 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 4.2

BRASÍLIA, 03 DE AGOSTO DE 2017

Sumário

Controle de Alterações

Versão	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. Revisão das funcionalidades do papel de acesso “usuário”. Inclusão do termo “Módulo criptográfico multiaplicação” no glossário.
3.0.r.50	22/11/07	Revisão geral para os requisitos de cartões criptográficos ICP-BRASIL 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-BRASIL, leitoras de cartões inteligentes e materiais a serem depositados para a execução do processo de homologação.
4.0	18/12/14	Revisão geral e reestruturação dos requisitos de cartões criptográficos ICP-Brasil resultante do GT Revisão dos MCTs.
4.1	18/04/2017	Inclusão das definições de Fronteira Criptográfica e Módulo Criptográfico.
4.2	03/08/2017	Previsão de autonomia para o OCP definir os ensaios nas Avaliações de Manutenção de Credenciamento; Ajuste na obrigatoriedade dos comandos APDU; e Retirada da obrigatoriedade de importação/exportação de certificados de atributo.

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 cartões criptográficos (*smartcards*) ICP no âmbito da Infraestrutura 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 Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1. Objetivo da homologação

O objetivo do processo de avaliação de conformidade é verificar a interoperabilidade e operação segura do cartão criptográfico ICP-BRASIL por meio da 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 no presente manual que devem ser atendidos por um cartão criptográfico ICP-BRASIL para prover interoperabilidade dos cartões através de sua padronização e operação segura de acordo com níveis de segurança previamente definidos, conforme descrito abaixo.

A versão atual deste manual considera dois possíveis níveis de segurança de homologação para cartões criptográficos ICP-Brasil.

Por questão de compatibilidade com as versões anteriores deste manual, optou-se por manter a denominação Nível 1 para o nível de homologação baseado em avaliação funcional e documental e Nível 3 para o nível de homologação baseado na análise das especificações completas e detalhadas do equipamento, inclusive de seu software.

- Nível 1: consiste em uma verificação de aderência através da análise funcional e documental. Este nível adiciona segurança limitada ao cartão, sendo aplicável quando

alguma confiança sobre sua correta operação é exigida, mas ameaças à segurança não apresentam maior gravidade.

- Nível 3: incorpora, adicionalmente aos requisitos de nível 1, uma verificação detalhada das características dos projetos de hardware e software, incluindo aspectos de implementação com base no código-fonte. Este nível representa um aumento significativo na segurança, utilizando procedimentos/mecanismos aperfeiçoados de análise a fim de proporcionar maior garantia de que o cartão não será adulterado.

Estes requisitos técnicos são avaliados pela execução de ensaios de aderência a estes requisitos. Para a realização destes ensaios, a parte interessada deve submeter ao processo de avaliação da conformidade um conjunto de materiais requisitados, efetuando o depósito destes materiais no LEA ou OCP acreditado.

A avaliação feita com base nos requisitos deste MCT não garante por si só a total segurança do sistema. O nível de segurança adequado ao cartão criptográfico deve ser escolhido de acordo com os requisitos da aplicação e do ambiente no qual o cartão será utilizado, assim como os serviços de segurança que o mesmo deverá oferecer.

1.3. Escopo deste manual

Os requisitos técnicos para os cartões criptográficos ICP-BRASIL são aplicados em todos os elementos/componentes (de software e hardware) envolvidos diretamente nas operações que envolvem manipulação dos certificados ICP-Brasil contidos no cartão.

Sendo assim, o escopo dos requisitos técnicos e da avaliação de cartões criptográficos ICP-BRASIL se aplica aos seguintes componentes do módulo criptográfico:

- Componentes eletrônicos (hardware).
- Sistema operacional embarcado (*Card Operating System* – COS).
- Funcionalidade PKI.
- Biblioteca de software disponível para comunicação com o cartão criptográfico ICP-BRASIL (*middleware*).

Em um Credenciamento Inicial e na Avaliação de Recertificação devem ser aplicados todos os ensaios definidos neste MCT. Em cada Avaliação de Manutenção, cabe ao OCP definir quais requisitos devem ser ensaiados. Uma Avaliação de Manutenção deve observar a proporção mínima de 20 (vinte) porcento do total dos requisitos previstos no Anexo I deste MCT para cada avaliação de manutenção no modelo 4 e de 33 (trinta e três) porcento do total dos

requisitos previstos no Anexo I deste MCT para cada avaliação de manutenção no modelo 5. A avaliação de um requisito em uma Avaliação de Manutenção não impede sua reavaliação em Avaliações de Manutenção seguintes, mas ao longo das Avaliações da Manutenção o OCP deve garantir que todos os requisitos do Anexo I sejam avaliados.

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-Brasil.
- Parte 2: Descreve os materiais que devem ser depositados para a execução do processo de homologação de cartões criptográficos ICP-Brasil.
- Referência Bibliográfica: Descreve as referências bibliográficas que foram utilizadas na elaboração deste manual.

2. Parte 1 - Requisito técnico para homologação de cartões criptográficos no âmbito da ICP-Brasil

Requisito técnico para homologação de cartões criptográficos no âmbito da 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-BRASIL.

2.1.1. Nomenclatura adotada para a identificação dos requisitos

A Tabela 1 apresenta a nomenclatura adotada para a classificação dos requisitos quanto aos seguintes grupos:

- Requisitos específicos para os manuais que acompanham o produto.
- Requisitos específicos para o *middleware*/funcionalidade PKI.
- Requisitos específicos para o módulo criptográfico.

Nomenclatura	Descrição
REQUISITO-DOC	Identifica os requisitos específicos para os manuais dos produtos.
REQUISITO-MC	Identifica os requisitos específicos do módulo criptográfico.
REQUISITO-MW	Identifica os requisitos específicos da *middleware*/funcionalidade PKI.

Tabela 1: Nomenclatura adotada para a identificação dos requisitos

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 [DOC-ICP-01.01].
- Requisitos de controle de acesso.
- Requisitos de identificação de hardware, software e *firmware*.

2.2.1. Controle de acesso

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.

DEFINIÇÃO: Mecanismos de controle de acesso 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 controle de acesso baseado em papéis tem como objetivo intermediar o acesso de usuário a um determinado serviço. A ideia central é que um usuário possa desempenhar diferentes papéis em um módulo criptográfico. Um papel pode ser definido como um conjunto de atividades e responsabilidades associados a um determinado cargo ou função.

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.

2.2.1.1. PIN

DEFINIÇÃO: O PIN (*Personal Identification Number*) é um código alfanumérico, inclusive caracteres especiais, sensível às maiúscula e minúscula (*case sensitive*) usado como chave para autenticar o usuário no sistema. Neste documento, o PIN será considerado como o mecanismo de identificação e autenticação do papel de acesso Usuário (*User*).

REQUISITO-MC II.1: O objeto em avaliação deve suportar, no mínimo, o papel de acesso Usuário com controle de acesso via PIN ou autenticação biométrica. O(s) papel(is) deve(m) suportar, no mínimo, o conjunto de serviços apresentados na Tabela 2.

Serviço Criptográfico	Usuário	Oficial de Segurança	Não-Autenticado
Gerar chave criptográfica assimétrica	X		
Excluir chave criptográfica assimétrica	X		
Recuperar parâmetros sobre uma determinada chave criptográfica assimétrica, tais como: algoritmo e atributos das chaves criptográficas.	X		
Importar cadeia de certificação para o módulo criptográfico	X		
Importar certificado digital para o módulo criptográfico	X		
Importar certificado digital de atributo para o módulo criptográfico	X		
Exportar chave criptográfica assimétrica pública do módulo criptográfico	X		X
Exportar certificado digital do módulo criptográfico	X		X
Exportar certificado digital de atributo do módulo criptográfico	X		X
Exportar cadeia de certificação do módulo criptográfico	X		X
Reinicialização do papel de acesso “Usuário”		X	
Desbloqueio do papel de acesso “Usuário”		X	
Alteração do PIN corrente do papel de acesso “Usuário”	X	X	
Alteração do PUK corrente do papel de acesso “Oficial de Segurança”		X	

Tabela 2: Relação entre serviços criptográficos e papéis de acesso

Observação: a coluna representada na tabela anterior com o rótulo “Não-Autenticado” expressa o papel de acesso no qual não há necessidade de autenticação de uma entidade usuária externa ao cartão criptográfico.

2.2.1.2. PUK

DEFINIÇÃO: O PUK (PIN *Unlock Key*) é um código alfanumérico, inclusive caracteres especiais, sensível às maiúscula e minúscula (*case sensitive*) 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-MC II.2: Dados de autenticação armazenados no interior do módulo criptográfico devem ser protegidos contra leitura, modificação, utilização e substituição não autorizada.

2.2.1.3. Qualidade dos códigos PIN e PUK

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

REQUISITO-MC II.3: A probabilidade de que uma única tentativa aleatória de autenticação com senha tenha sucesso deve ser inferior a 1 em 1.000.000. Em autenticação por biometria, a especificação mínima de precisão deve estar em conformidade com o NIST SP 800-76-2:2013 do padrão FIPS 201-2:2013.

REQUISITO-MC II.4: Caso o objeto em avaliação possua o recurso de autenticação biométrica, este deve seguir os requisitos de autenticação por métodos biométricos para um cartão criptográfico conforme definido no padrão ISO/IEC 7816-11:2004.

2.2.2. 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-MC II.5: O modelo de estado finito do objeto em avaliação deve descrever os estados de autoteste e os estados de erro.

2.2.3. 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-MC II.6: Os circuitos integrados presentes no cartão criptográfico devem ser protegidos por invólucros (cobertura ou revestimento) que evidenciem violações físicas. No mínimo, um cartão criptográfico deve possuir dois invólucros de proteção: plástico PVC (invólucro de proteção mais externo) e resina com pigmentação utilizada para recobrir seu circuito integrado (invólucro de proteção mais interno, como por exemplo, epóxi pigmentado). Sua finalidade é deter a observação, sondagem visual do chip e seus componentes ou manipulação dos dados sem que haja a remoção dos invólucros, provendo evidências sobre tentativas de violar, obter acesso ou remover os componentes protegidos.

2.2.4. 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-MC II.7: Chaves simétricas, chaves assimétricas privadas e PCS devem estar protegidas dentro do módulo criptográfico contra leitura, modificação, utilização e substituição não autorizada.

REQUISITO-MC II.8: Chaves públicas devem estar protegidas dentro do módulo criptográfico contra modificação e substituição não autorizada.

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

REQUISITO-MC II.9: Somente algoritmos RNG determinísticos aprovados pela família de padrões FIPS devem ser usados pelo módulo criptográfico para geração de chaves criptográficas (Figura 1).

REQUISITO-MC II.10: Algoritmos RNG (aprovados ou não pela família de padrões FIPS) podem ser usados para a geração de vetores de iniciação (IV) de algoritmos criptográficos, exceto para os modos de operação CBC e CFB, os quais obrigatoriamente devem ter seus respectivos vetores de iniciação gerados por meio de algoritmos RNG determinísticos aprovados pela família de padrões FIPS (Figura 1).

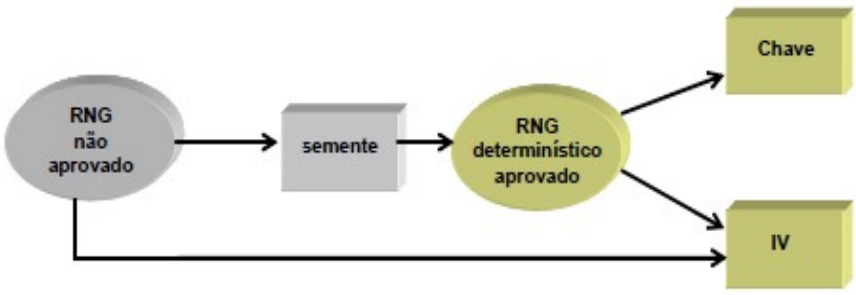

Figura 1: Geradores de números aleatórios

2.2.4.2. Geração de chaves criptográficas

REQUISITO-MC II.11: O módulo criptográfico deve usar para a geração de chaves criptográficas obrigatoriamente uma das duas opções seguintes: o resultado de um RNG aprovado pela família de padrões FIPS, ou então métodos específicos de geração de chaves criptográficas aprovados pela família de padrões FIPS. Caso seja necessário que um método específico de geração de chaves criptográficas utilize como entrada o resultado de um RNG, então o RNG utilizado deve ser aprovado pela família de padrões FIPS.

2.2.4.3. 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-MC II.12: Se métodos de transporte de chaves criptográficas são suportados pelo módulo criptográfico, então somente os métodos e algoritmos aprovados pela família de padrões FIPS devem ser usados.

2.2.4.4. 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-MC II.13: Se o módulo criptográfico permitir a importação de PCS (chaves simétricas, chaves assimétricas privadas e dados de autenticação), então os PCS devem ser importados no módulo de forma cifrada 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-MC II.14: Chaves criptográficas assimétricas privadas devem ser configuradas no módulo criptográfico somente de forma não exportável. O módulo criptográfico deve vedar a exportação de chaves criptográficas assimétricas privadas.

REQUISITO-MC II.15: O objeto em avaliação deve implementar métodos de sobrescrita dos valores de PCS (chaves criptográficas e dados de autenticação).

2.2.5. Algoritmos criptográficos obrigatórios

REQUISITO-MC II.16: Com relação aos algoritmos criptográficos obrigatórios suportados no objeto em avaliação, devem ser considerados aqueles aplicáveis definidos na versão corrente do documento denominado "PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01)".

REQUISITO-MC II.17: No módulo criptográfico, o uso de chaves simétricas e assimétricas privadas deve ser habilitado apenas nos casos de autenticação bem-sucedida do papel de acesso Usuário.

REQUISITO-MC II.18: O módulo criptográfico deve ter função específica para alterar o PIN corrente que habilita acesso ao papel usuário. O novo valor do PIN somente deve ser alterado com autenticação do PIN corrente ou do PUK (caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança).

REQUISITO-MC II.19: 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 malsucedidas.

REQUISITO-MC II.20: O módulo criptográfico deve ter controle para forçar que, no primeiro acesso, o proprietário do cartão criptográfico altere o PIN padrão de inicialização.

REQUISITO-MC II.21: O módulo criptográfico deve ser reinicializado mediante inserção correta do PUK pela entidade usuária externa e ao ser reinicializado prover a eliminação do valor do PIN e de todas as chaves criptográficas secretas associadas ao papel de acesso "Usuário". Após ser reinicializado, o módulo criptográfico deve estar disponível para reutilização. Requisito aplicável caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança.

REQUISITO-MC II.22: O módulo criptográfico deve permitir ao usuário, após informar corretamente o PUK, o desbloqueio do papel de acesso Usuário, mediante a inserção de um novo PIN. Requisito aplicável caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança.

REQUISITO-MC II.23: O módulo criptográfico deve permitir ao usuário a troca do PIN mediante a inserção do novo PIN após a autenticação bem-sucedida do usuário.

REQUISITO-MC II.24: 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 malsucedidas. Requisito aplicável caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança.

REQUISITO-MC II.25: 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. Requisito aplicável caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança.

2.2.5.1. Cache das credenciais de autenticação

O "Provedor de Serviços" (PS) pode realizar o cache 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-MW II.26: O código PUK nunca deve ser mantido em cache pela middleware. Requisito aplicável caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança.

REQUISITO-MW II.27: Sempre que realizar cache (armazenamento temporário em memória), a middleware deve manter o valor do PIN de forma protegida (valor do PIN disponível apenas no momento de seu uso) contra observação direta. Uma vez em cache, o valor do PIN deve ser eliminado sempre que ocorra as seguintes situações:

- Sempre que a alimentação elétrica do módulo criptográfico for retirada.
- Sempre que a aplicação de usuário associada ou conectada ao módulo for encerrada.
- E, caso seja possível configurar o tempo de duração máxima do PIN no cache (Time To Live – TTL), sempre que o TTL for expirado.

2.2.5.2. Sobrescrita do valor de chaves criptográficas

REQUISITO-MW II.28: A eliminação do código PIN presente no cache deve ser realizada com sobrescrita de seu valor.

REQUISITO-MW II.29: No contexto e controle específico interno da middleware, o tamanho mínimo dos valores de PIN (bem como PUK, caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança) deve ser igual a 4 posições considerando caracteres alfanuméricos sensíveis a letras maiúsculas e minúsculas (case sensitive).

2.3. Requisitos de Interoperabilidade

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.

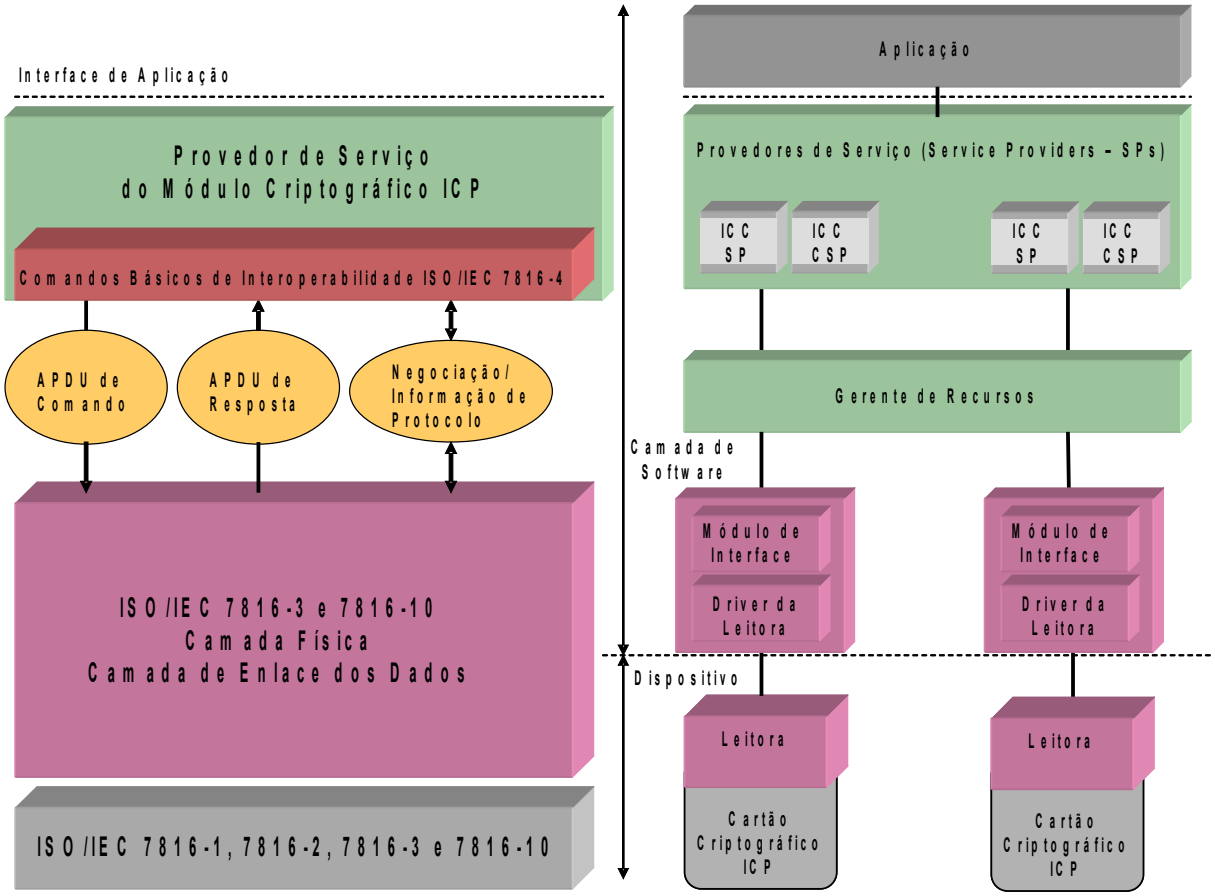

Figura 2. Arquitetura de interoperabilidade de cartões ISO 7816 e PC/SC

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

- 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 poderão ser realizados em diferentes plataformas e

versões de sistemas operacionais atualmente disponíveis (tais como, Microsoft Windows, Linux e UNIX).

2.3.2. 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-MC III.1: Um módulo criptográfico deve seguir uma estrutura de comandos e respostas APDU (Application Protocol Data Unit) conforme os requisitos e as convenções definidas no padrão ISO/IEC 7816-4:2005.

2.3.3. Conjunto mínimo de comandos

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, e define a obrigatoriedade do atendimento a um conjunto mínimo de comandos.

REQUISITO-MC III.2: Um módulo criptográfico deve suportar, no mínimo, o conjunto de comandos apresentados na Tabela 3.

Comando	Definição e escopo	Exemplo (ISO 7816-4)
1	Comando para leitura de dados de um arquivo binário, iniciando a leitura de uma posição (offset) especificada por um parâmetro passado via comando.	**READ BINARY**
2	Comando para recuperar ou ler objetos de dados.	**GET DATA**
3	Comando para armazenar ou escrever objetos de dados.	**PUT DATA**
4	Comando para selecionar um arquivo.	**SELECT FILE**
5	Comando para comparar um segredo enviado via interface (PIN, por exemplo) com um valor de referência já armazenado no módulo criptográfico.	**VERIFY**
6	Comando para autenticar uma entidade externa perante um módulo criptográfico.	**EXTERNAL AUTHENTICATE**
7	Comando para requerer do módulo criptográfico um número randômico (desafio – "challenge") para ser usado posteriormente para fins de autenticação.	**GET CHALLENGE**

Tabela 3: Conjunto mínimo de comandos para módulos criptográficos

2.3.4. Requisitos de gerenciamento de aplicações no módulo criptográfico

REQUISITO-MC III.3: O objeto em avaliação deve seguir os requisitos de ciclo de vida para um cartão criptográfico conforme definido no padrão ISO/IEC 7816-9:2004.

REQUISITO-MC III.4: O objeto em avaliação deve seguir os requisitos de gestão de aplicações para um cartão criptográfico multiaplicação conforme definido no padrão ISO/IEC 7816-13:2007.

2.3.5. Dimensões de contatos elétricos de cartões criptográficos ICP-BRASIL

REQUISITO-MC III.5: Um cartão criptográfico com contato deve possuir dimensões compatíveis com aquelas definidas pelo padrão ISO/IEC 7810 e também atender aos requisitos definidos nos padrões ISO/IEC 7816-1:2003 e ISO/IEC 7816-2:2007.

2.3.6. Requisitos de interface física

2.3.6.1. Atribuição de contatos elétricos

REQUISITO-MC III.6: Contatos não utilizados, caso estejam presentes no cartão criptográfico, devem ser identificados e isolados, do ponto de vista elétrico (não condutíveis), do CI (Circuito Integrado) e de quaisquer outros contatos inseridos no cartão.

2.3.6.2. Propriedades elétricas

REQUISITO-MC III.7: Um cartão criptográfico com interface de contato deve atender os requisitos de interface elétrica e de protocolos de transmissão definidos na norma ISO/IEC 7816-3:2006.

REQUISITO-MC III.8: Caso o cartão criptográfico possua interface sem contato, o objeto em avaliação deve seguir os requisitos definidos na família de padrões ISO/IEC 14443.

2.4. 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-MW 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 (Next Generation).
- PKCS#11.
- JCE.
- OpenSSL.

2.4.1. Gerenciamento de chaves criptográficas

REQUISITO-MW IV.2: Os seguintes requisitos funcionais de gestão de chaves criptográficas devem estar disponíveis por invocação via middleware:

- Gerar chave criptográfica assimétrica no módulo criptográfico.
- Excluir chave criptográfica assimétrica.
- Recuperar parâmetros sobre uma determinada chave criptográfica assimétrica, tais como: algoritmo e atributos das chaves criptográficas.

2.4.2. Exportação e importação de chaves criptográficas

REQUISITO-MW IV.3: Os seguintes requisitos funcionais de exportação e importação devem estar disponíveis por invocação via *middleware*:

- Importar cadeia de certificação para o módulo criptográfico.
- Importar certificado digital para o módulo criptográfico.
- Exportar chave criptográfica assimétrica pública do módulo criptográfico.
- Exportar certificado digital do módulo criptográfico.
- Exportar cadeia de certificação do módulo criptográfico.

Observação: A Parte Interessada deve informar os atributos das chaves assimétricas e dos certificados digitais utilizados na importação.

REQUISITO-MW IV.4: Em seu contexto específico, a middleware deve possibilitar a configuração segura de chaves simétricas, chaves assimétricas privadas e PCS de tal forma a estarem protegidas contra leitura, modificação, utilização e substituição não autorizada.

REQUISITO-MW IV.5: Em seu contexto específico, a middleware deve possibilitar a configuração segura de chaves assimétricas públicas de tal forma a estarem protegidas contra modificação e substituição não autorizada.

REQUISITO-MW IV.6: Dentro de seu escopo específico, a middleware deve possuir a funcionalidade de propagar automaticamente os certificados digitais contidos em um cartão criptográfico para um repositório de certificados digitais que pode ser lido por aplicações de usuários (por exemplo, browsers, softwares de assinatura digital etc.). De forma complementar, ao propagar automaticamente certificados digitais para um repositório, a

middleware deve prover rotinas ou funcionalidades adicionais necessárias para a interação entre aplicação de usuário e cartão criptográfico e que sejam compatíveis com o sistema operacional alvo da avaliação.

2.5. 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-DOC V.1: O objeto em avaliação deve fornecer, no mínimo, as seguintes informações, em idioma português do Brasil, em um ou mais manuais que acompanham o produto na sua forma comercial:

- Instalação da middleware.
- Plataformas de sistemas operacionais compatíveis.
- Versão completa dos componentes de software do produto.

Observação: Por versão completa do software entende-se a versão do componente principal de software acompanhado da versão de todos os componentes derivados de software.

REQUISITO-DOC V.2: O fabricante do objeto em avaliação deve demonstrar que tomou as devidas precauções no sentido de evitar a ocorrência de vulnerabilidades típicas de segurança.

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**

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 ou OCP acreditado para a execução dos processos de homologação de cartões criptográficos ICP-BRASIL (*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-BRASIL 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*).

Dois 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 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 o NSH 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-BRASIL, 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 OCP:

M1 Cartão criptográfico ICP-BRASIL de produção.

M2 Cartão criptográfico ICP-BRASIL de teste.

OBSERVAÇÃO: Amostras nas quantidades definidas por este documento para cada modelo e/ou versão de cartão criptográfico ICP-BRASIL 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 ou OCP acreditado, pela parte interessada:

M3 Identificação de componentes: elementos que permitam a identificação das versões e revisões dos seguintes componentes:

- ✔ Hardware: fabricante, modelo e versão do CI (Circuito Integrado).
- ✔ Firmware: versão completa do COS (Card Operating System) e versão do aplicativo ICP-BRASIL.
- ✔ Software: os seguintes parâmetros para cada componente da versão completa da middleware.: número da versão, data da última modificação, nome do fabricante ou responsável e descrição da finalidade.
- ✔ ATR: deverá identificar univocamente o cartão criptográfico ICP-BRASIL.

OBSERVAÇÃO: Por versão completa entende-se a versão do componente principal acompanhado da versão de todos os componentes derivados.

M4 **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-BRASIL 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.

M5 **Política de segurança:** Política de segurança utilizada para o objeto de homologação constando, no mínimo, as seguintes seções:

- ✔ Introdução.
- ✔ Especificação do módulo criptográfico.
- ✔ Portas e interfaces do módulo criptográfico.
- ✔ Papéis, serviços e autenticação.
- ✔ Segurança lógica (software security).
- ✔ Ambiente operacional.
- ✔ Segurança física.
- ✔ Segurança física contra ataques não invasivos.
- ✔ Gerenciamento de dados sensíveis (chaves criptográficas e dados de autenticação).
- ✔ Autotestes.
- ✔ Mitigação de outros ataques.

M6 **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-Brasil;
- ✔ 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.

M7 **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.

M8 **Relação de certificados obtidos**: Relação de certificação e/ou licenças obtidas para o módulo criptográfico emitidas por entidades independentes.

M9 **Documentação adicional sobre o módulo criptográfico:** As seguintes informações também devem estar descritas na documentação que é depositada para a análise de conformidade:

DEFINIÇÃO: Um módulo criptográfico é um conjunto de hardware, software e *firmware*, ou uma combinação disso que implementa funções criptográficas ou processos, incluindo algoritmos criptográficos e opcionalmente geração de chaves criptográficas. É contido dentro de uma fronteira criptográfica bem definida, portanto é importante saber de cada componente do conjunto e o que passa na fronteira criptográfica como entrada e saída de dados e valores sigilosos.

DEFINIÇÃO: A fronteira criptográfica é um perímetro explicitamente definido que estabelece os limites físicos de um módulo criptográfico. Se um módulo criptográfico for composto por componentes de software ou firmware, a fronteira criptográfica deve conter o(s) processador(es) e outros dispositivos de hardware que armazenam e protegem os componentes de software e firmware. Componentes de hardware, software e firmware do módulo criptográfico podem ser excluídos dos requisitos apresentados neste documento, caso tais componentes não afetem a segurança do módulo.

- ✔ Módulo criptográfico:
  - ✔ componentes de hardware, software e firmware do módulo criptográfico, incluindo suas respectivas versões;
  - ✔ qualquer componente de hardware, software ou firmware que seja excluído dos requisitos de segurança;
  - ✔ configuração física do módulo;
  - ✔ características elétricas, lógicas e físicas aplicáveis ao módulo;

- identificação dos contatos elétricos que são utilizados pelos cartões criptográficos ICP-Brasil.
- quando utilizado o contato elétrico C6, justificativa da necessidade de uso;
- funções de segurança e operações criptográficas que são empregadas pelo módulo, assim como todos os modos de operação suportados;
- datasheet completo do hardware com descrição dos blocos internos que fazem parte do circuito integrado.
- diagrama de blocos funcional do hardware.
- descrição da fronteira criptográfica.
- diagrama de blocos funcional ou arquitetura do sistema operacional embarcado.
- arquitetura do software embarcado que implementa funcionalidades de PKI.
- indicação do modelo e da versão do circuito integrado.
- forma de organização de arquivos e estrutura de dados utilizada pelo 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 críticos de segurança (PCS).
- 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;

- 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.
  - métodos de atribuição de chaves empregados pelo módulo criptográfico.

- Geradores de números aleatórios (*Random Number Generators* – RNG):
  - Cada RNG e Pseudo 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 públicas 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:
  - Autotestes de energia:
    - Teste de algoritmo criptográfico.
    - Teste de integridade de software/firmware.
    - Teste de funções críticas.
    - Outros autotestes que são executados na energização.
  - Autotestes condicionais:
    - Teste de consistência de par de chaves (pairwise).
    - Teste de integridade de software/firmware.
    - Teste de gerador de números aleatórios contínuo.
    - Outros 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.

M10 Manuais que acompanham o produto na sua forma comercial:

- ✔ Instalação da *middleware*.
- ✔ Plataformas de sistemas operacionais compatíveis.
- ✔ Versão completa dos componentes de software do produto.

OBSERVAÇÃO: Por versão completa do software entende-se a versão do componente principal de software acompanhado da versão de todos os componentes derivados de software.

M11 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 3

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

M12 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*.

M13 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 ou OCP acreditado:

M14 Provedor(es) de serviço criptográfico: Provedor(es) de serviço criptográfico, para as arquiteturas de hardware e para os sistemas operacionais suportados.

M15 Ferramenta de gerenciamento do módulo criptográfico.

M16 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-BRASIL que se resumem em:

- Componentes físicos: amostras de cada modelo e/ou versão de cartão criptográfico ICP-BRASIL;
- 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 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 ou OCP acreditado, referente ao processo de homologação de cartão criptográfico ICP-Brasil.

Requisito de depósito	Material e documentos técnicos a serem depositados pela parte interessada – NSH 1	Quantidade
M1	Cartão criptográfico ICP-BRASIL de produção	7 unidades
M2	Cartão criptográfico ICP-BRASIL de teste	3 unidades
M3	Identificação de Componentes	
M4	PIN e PUK padrão	
M5	Política de segurança	2 cópias
M6	Documentação que acompanha o produto	2 cópias
M7	Manual de comandos APDU suportados	2 cópias
M8	Relação de certificados obtidos	2 cópias
M9	Documentação adicional sobre o módulo criptográfico	2 cópias
M10	Manuais que acompanham o produto na sua forma comercial	2 cópias
M11	Outros documentos	2 cópias
Requisito de depósito	**Material e documentos técnicos a serem depositados pela parte interessada – NSH 3**	**Quantidade**
M12	Código fonte embarcado	2 cópias
M13	Código fonte de apoio	2 cópias
Requisito de depósito	**Componentes em software executável a serem depositados pela parte interessada – NSH 1 e 3**	**Quantidade**
M14	Provedor(es) de serviço criptográfico	2 cópias
M15	Ferramenta de gerenciamento do módulo criptográfico	2 cópias
M16	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] INFRAESTRUTURA 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.

[DOC-ICP-01.01] PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL – Aprovada pela RESOLUÇÃO Nº 89, DE 05 DE JULHO DE 2012.

ANEXO I

Requisitos para a Avaliação de Manutenção

REQUISITO	Quantidade de ensaios
REQUISITO-MC II.1	2
REQUISITO-MC II.2	3
REQUISITO-MC II.3	4
REQUISITO-MC II.4	3
REQUISITO-MC II.5	2
REQUISITO-MC II.6	2
REQUISITO-MC II.7	4
REQUISITO-MC II.8	3
REQUISITO-MC II.9	3
REQUISITO-MC II.10	3
REQUISITO-MC II.11	3
REQUISITO-MC II.12	2
REQUISITO-MC II.13	3
REQUISITO-MC II.14	3
REQUISITO-MC II.15	2
REQUISITO-MC II.16	4
REQUISITO-MC II.17	6
REQUISITO-MC II.18	4
REQUISITO-MC II.19	3
REQUISITO-MC II.20	3
REQUISITO-MC II.21	4
REQUISITO-MC II.22	3
REQUISITO-MC II.23	3
REQUISITO-MC II.24	3
REQUISITO-MC II.25	3
REQUISITO-MC III.5	2
REQUISITO-MC III.6	3