Manual de Condutas Técnicas 1 - Volume II

Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos de Cartões Criptográficos (*Smart Cards*) no Âmbito da ICP-Brasil

Versão 4.1

BRASÍLIA, 18 DE ABRIL DE 2017

Sumário

CONTROLE DE ALTERAÇÕES....4
LISTAS DE ILUSTRAÇÕES....5
1. INTRODUÇÃO....6
1.1.Objetivo da homologação....6
1.2.Organização deste Documento....6
1.3.Estruturação do MCT 1 – Volume II....7
2.PARTE 1 – PROCEDIMENTOS DE ENSAIOS PARA HOMOLOGAÇÃO DE CARTÕES CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL....8
2.1.Introdução....9
2.1.1.Nomenclatura adotada para a identificação dos requisitos....9
2.2.Requisitos de Segurança....9
2.2.1.Controle de acesso....9
2.2.1.1.PIN....10
2.2.1.2.PUK....12
2.2.1.3.Qualidade dos códigos PIN e PUK....13
2.2.2.Modelo de estado finito....14
2.2.3.Segurança física....15
2.2.4.Gerenciamento de chaves criptográficas....16
2.2.4.1.Geradores de números aleatórios (Random Number Generators - RNG)....18
2.2.4.2.Geração de chaves criptográficas....20
2.2.4.3.Atribuição de chaves....21
2.2.4.4.Importação e exportação de chaves criptográficas....22
2.2.5.Algoritmos criptográficos obrigatórios....24
2.2.5.1.Cache das credenciais de autenticação....32
2.2.5.2.Sobrescrita do valor de chaves criptográficas....34
2.3.Requisitos de Interoperabilidade....36
2.3.1.Módulo criptográfico....36
2.3.2.Estrutura da mensagem de APDU....38
2.3.3.Conjunto mínimo de comandos....38
2.3.4.Requisitos de gerenciamento de aplicações no módulo criptográfico....40
2.3.5.Dimensões de contatos elétricos de cartões criptográficos ICP-BRASIL....41

2.3.6.Requisitos de interface física....41
2.3.6.1.Atribuição de contatos elétricos....41
2.3.6.2.Propriedades elétricas....42
2.4.Requisitos funcionais....43
2.4.1.Gerenciamento de chaves criptográficas....43
2.4.2.Exportação e importação de chaves criptográficas....44
2.5.Requisitos de documentação....49
3.REFERÊNCIAS BIBLIOGRÁFICAS....51

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.

Listas de Ilustrações

Lista de Figuras

Figura 1: Geradores de números aleatórios.....19
Figura 2. Arquitetura de interoperabilidade de cartões ISO 7816 e PC/SC.....37

Lista de Tabelas

Tabela 1: Nomenclatura adotada para a identificação dos requisitos.....9
Tabela 2: Relação entre serviços criptográficos e papéis de acesso.....11
Tabela 3: Conjunto mínimo de comandos para módulos criptográficos.....40

1. Introdução

Este documento descreve os procedimentos de ensaios a serem aplicados no processo de homologação de cartões criptográficos (*smartcards*) no âmbito da Infraestrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Os procedimentos de ensaio se referem ao conjunto de métodos que serão usados para avaliar se cartões criptográficos estão ou não em conformidade com os requisitos técnicos definidos pelo Manual de Condutas Técnicas 1 - Volume I.

Para uma melhor compreensão do disposto neste documento, entenda-se por cartão criptográfico 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 por meio da aderência aos requisitos técnicos definidos neste manual.

1.2. Organização deste Documento

Cada seção deste documento contém um conjunto de requisitos que representam citações diretas do próprio texto do Manual de Condutas Técnicas 1 – Volume I. Os requisitos estão organizados da seguinte forma:

- REQUISITO <número_do_requisito>.<número_de_seqüência_do_requisito>
  - "número_do_requisito": corresponde ao número de área definido no Manual de Condutas Técnicas 1 – Volume I;
  - "número_de_sequência_do_requisito": corresponde a um identificador sequêncial dos requisitos.

Os procedimentos de ensaio visam a orientar sobre como proceder nos testes elaborados sobre dispositivos. Os procedimentos de ensaio estão classificados e agrupados por Níveis de Segurança de Homologação. A versão atual deste manual considera dois possíveis níveis de segurança de homologação para cartões criptográficos no âmbito da 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.

- 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.

Os procedimentos de ensaio (EN) que devem ser desempenhados pelo analista do LEA ou OCP estão organizados da seguinte forma:

- EN.<número_do_requisito>.<número_de_sequência_do_requisito>.<número_de_sequência_do_ensaio>
  - "número_do_requisito";
  - "número_de_sequência_do_requisito";
  - "número_de_sequência_do_ensaio": corresponde a um identificador sequêncial dos procedimentos que devem ser desempenhados

1.3. Estruturação do MCT 1 – Volume II

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

- Parte 1: Descreve os procedimentos de ensaios que devem ser verificados no processo de homologação de cartões criptográficos ICP-Brasil.
- Referência Bibliográfica: Descreve as referências bibliográficas que foram utilizadas na elaboração deste manual.

2. Parte 1 – Procedimentos de Ensaios para homologação de cartões criptográficos no âmbito da ICP-Brasil

Procedimentos de ensaios para homologação de cartões criptográficos no âmbito da ICP-Brasil

2.1. Introdução

A parte 1 deste documento apresenta os procedimentos de ensaios 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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.1.1: Para cada papel de acesso suportado pelo módulo criptográfico, realizar testes executando todos os serviços associados ao papel de acesso assumido, verificando se há consistência com os papéis de acesso e serviços descritos na documentação técnica fornecida.

Procedimentos de ensaio para NSH 3.

EN.II.1.2: Por meio de inspeção do código fonte do software embarcado, verificar como o módulo criptográfico realiza a associação entre papéis de acesso suportados e serviços oferecidos.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.2.1: Tentar obter acesso aos dados de autenticação para os quais não está autorizado, utilizando comandos APDU. O módulo deve proibir que os dados de autenticação sejam visualizados no formato de texto legível.

EN.II.2.2: Tentar modificar ou substituir dados de autenticação para os quais não está autorizado, utilizando comandos APDU. O módulo deve proibir que os dados de autenticação sejam modificados ou substituídos sem o devido controle.

Procedimentos de ensaio para NSH 3.

EN.II.2.3: Por meio de inspeção do código fonte do software embarcado, verificar como o módulo criptográfico proíbe que os dados de autenticação sejam modificados ou substituídos sem o devido controle.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.3.1: No caso de autenticação por biometria, estimar experimentalmente as especificações mínimas de precisão em conformidade com o NIST SP 800-76-2:2013, que complementa o padrão FIPS 201-2:2013.

EN.II.3.2: No caso de autenticação por senha (incluindo PIN e PUK), tentar definir uma senha com tamanho inferior a 4 bytes por meio de comandos APDU. O módulo deve proibir a atribuição de valores de PIN e/ou PUK menores que 4 bytes.

EN.II.3.3: No caso de autenticação por senha (incluindo PIN e PUK), estimar, por meio de análise de documentação e por meio de comandos APDU, que o conjunto de senhas possíveis tem cardinalidade pelo menos 1.000.000.

Procedimentos de ensaio para NSH 3.

EN.II.3.4: Por meio de inspeção do código fonte do software embarcado, verificar como o módulo criptográfico garante que a política de autenticação definida neste requisito seja cumprida.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.4.1: Verificar por meio de documentação técnica fornecida pela parte interessada se os requisitos de autenticação por métodos biométricos para um cartão criptográfico estão em conformidade com a norma ISO/IEC 7816-11:2004.

EN.II.4.2: Realizar testes para verificar se os requisitos de autenticação por métodos biométricos para um cartão criptográfico estão aderentes à norma ISO/IEC 7816-11:2004.

Procedimentos de ensaio para NSH 3.

EN.II.4.5: Por meio de análise do código fonte do software embarcado, verificar se os requisitos de autenticação biométrica estão de acordo com a documentação fornecida.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.5.1: Analisar a documentação técnica e verificar se a mesma contém uma descrição do modelo de estado finito. Esta descrição deve conter a identificação e detalhamento dos estados de autoteste e os estados de erro.

Procedimentos de ensaio para NSH 3.

EN.II.5.2: Por meio de inspeção do código fonte, verificar a consistência entre o modelo de estado finito implementado e o modelo documentado.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.6.1: Realizar tentativas de penetração física no invólucro de proteção mais externo utilizando bisturi e/ou outras ferramentas de corte, de forma a causar o mínimo possível de evidência de violação. Após tentativas de penetração verificar se o invólucro de proteção mais externo produziu evidências suficientes para comprovar que houve tentativa de violação.

EN.II.6.2: Realizar tentativas de sondagem ou observação no invólucro de proteção mais interno por meio de técnicas específicas e verificar se qualquer informação pode ser obtida a respeito do módulo criptográfico (como por exemplo, disposição dos componentes físicos).

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.7.1: Analisar a documentação técnica e verificar como o módulo criptográfico protege chaves simétricas, chaves assimétricas privadas e PCS contra leitura, modificação, utilização e substituição não autorizada.

EN.II.7.2: Tentar obter acesso às chaves simétricas, chaves assimétricas privadas e PCS para os quais não está autorizado, utilizando comandos APDU. O módulo deve proibir que as chaves simétricas, chaves assimétricas privadas e PCS sejam visualizados no formato de texto legível.

EN.II.7.3: Tentar modificar ou substituir chaves simétricas, chaves assimétricas privadas e PCS para os quais não está autorizado, utilizando comandos APDU. O módulo deve proibir que chaves simétricas, chaves assimétricas privadas e PCS sejam modificados ou substituídos sem o devido controle.

Procedimentos de ensaio para NSH 3.

EN.II.7.4: Por meio de análise do código fonte do software embarcado, verificar como o módulo criptográfico proíbe que chaves simétricas, chaves assimétricas privadas e PCS sejam modificados ou substituídos sem o devido controle.

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

Procedimentos de ensaio para NSH 1 e 3.

EN.II.8.1: Analisar a documentação técnica e verificar como o módulo criptográfico protege chaves assimétricas públicas contra modificação e substituição não autorizada.

EN.II.8.2: Tentar modificar ou substituir chaves assimétricas públicas para os quais não está autorizado, utilizando comandos APDU. O módulo deve proibir que chaves assimétricas públicas sejam modificadas ou substituídas sem o devido controle.

Procedimentos de ensaio para NSH 3.

EN.II.8.3: Por meio de análise do código fonte do software embarcado, verificar como o módulo criptográfico proíbe que chaves assimétricas públicas sejam modificadas ou substituídas sem o devido controle.

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).

Procedimentos de ensaio para NSH 1 e 3.

EN.II.9.1: Analisar a documentação técnica e verificar quais são os algoritmos RNG determinísticos utilizados pelo módulo criptográfico, e ainda, se tais algoritmos são aprovados ou não pela família de padrões FIPS. Algoritmos aprovados são listados no FIPS 140-2 anexo C.

EN.II.9.2: Por meio de ferramenta experimental que utiliza uma interface disponibilizada pela PI (por exemplo, API), realizar testes que permitam verificar o comportamento estatístico dos algoritmos RNG determinísticos suportados pelo módulo criptográfico. Caso não exista algum tipo de interface que permita a realização deste ensaio, o algoritmo será avaliado nos ensaios previstos para NSH 3.

Procedimentos de ensaio para NSH 3.

EN.II.9.3: Por meio de análise do código fonte do software embarcado, verificar se o algoritmo implementado RNG determinístico aprovado pela família de padrões FIPS é utilizado para geração de chaves ou para geração de vetores de iniciação definidos em algoritmos criptográficos.

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).

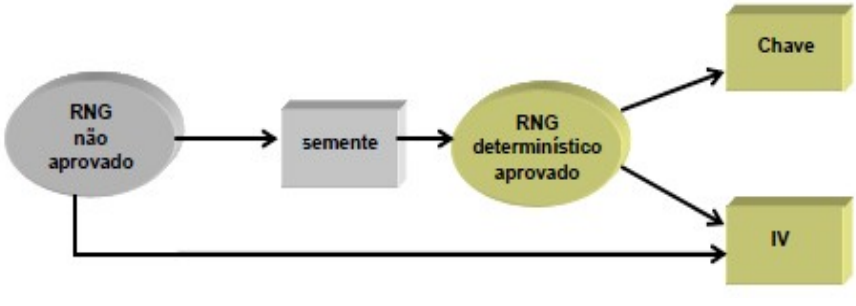

Figura 1: Geradores de números aleatórios

Procedimentos de ensaio para NSH 1 e 3.

EN.II.10.1: Analisar a documentação técnica e verificar quais são os algoritmos RNG não aprovados pela família de padrões FIPS utilizados pelo módulo criptográfico, como por exemplo, geradores tipo TRNG em hardware.

EN.II.10.2: Por meio de ferramenta experimental que utiliza uma interface disponibilizada pela PI (por exemplo, API), realizar testes que permitam verificar o comportamento estatístico dos algoritmos RNG não aprovados pela família de padrões FIPS suportados pelo módulo criptográfico. Caso não exista algum tipo de interface que permita a realização deste ensaio, o algoritmo será avaliado nos ensaios previstos para NSH 3.

Procedimentos de ensaio para NSH 3.

EN.II.10.3: Por meio de análise do código fonte do software embarcado, verificar se o algoritmo implementado RNG não aprovado pela família de padrões FIPS, é utilizado somente para geração de sementes para algoritmos RNG determinísticos aprovados pela família de padrões FIPS ou para geração de vetores de iniciação (exceto para os modos de operação CBC e CFB, os quais obrigatoriamente devem utilizar gerados de números aleatórios aprovados pela família de padrões FIPS).

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.11.1: Analisar a documentação técnica e verificar quais são os métodos de geração de chaves criptográficas usados pelo módulo criptográfico, e ainda, se tais métodos são ou não aprovados pela família de padrões FIPS.

EN.II.11.2: Por meio de ferramenta experimental que utiliza uma interface disponibilizada pela PI (por exemplo, API), realizar testes que permitam verificar se os métodos de geração de chaves criptográficas suportados pelo módulo criptográfico são algoritmos aprovados pela família de padrões FIPS. Caso não exista algum tipo de interface que permita a realização deste ensaio, o algoritmo será avaliado nos ensaios previstos para NSH 3.

Procedimentos de ensaio para NSH 3.

EN.II.11.3: Por meio de análise do código fonte do software embarcado, verificar se somente métodos aprovados pela família de padrões FIPS são usados para geração de chaves criptográficas. Além disso, verificar também se os métodos de geração de chaves criptográficas aprovados pela família de padrões FIPS, quando necessitarem como entrada o resultado de um algoritmo RNG, utilizam somente algoritmos RNG aprovados 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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.12.1: Analisar a documentação técnica e verificar quais são os métodos de transporte de chaves criptográficas suportados pelo módulo criptográfico e ainda, se tais algoritmos constam no anexo D do FIPS PUB 140-2.

Procedimentos de ensaio para NSH 3.

EN.II.12.2: Por meio de análise do código fonte do software embarcado, verificar se somente métodos de transporte de chaves aprovados pela família de padrões FIPS são 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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.13.1: Analisar a documentação técnica e verificar como os processos de importação são realizados para chaves criptográficas simétricas, assimétricas privadas e dados de autenticação.

EN.II.13.2: Verificar no módulo criptográfico por meio da técnica de captura do fluxo de comunicação de dados, se no processo de importação de chave assimétrica privada, chave simétrica e dados de autenticação não ocorre tráfego em claro e apresenta proteção com emprego de criptografia, em concordância com o apresentado na documentação analisada.

Procedimentos de ensaio para NSH 3.

EN.II.13.3: Por meio de análise do código fonte do software embarcado, verificar se o processo de importação de chaves criptográficas simétricas, assimétricas privadas e dados de autenticação, utiliza algoritmo aprovado pela família de padrões FIPS.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.14.1: Analisar a documentação técnica e verificar como o módulo criptográfico impede a exportação de chaves criptográficas assimétricas privadas.

EN.II.14.2: Tentar exportar chave criptográfica assimétrica privada do módulo criptográfico. O módulo criptográfico deve proibir a exportação de chaves criptográficas assimétricas privadas.

Procedimentos de ensaio para NSH 3.

EN.II.14.3: Por meio de análise do código fonte do software embarcado, verificar como o mecanismo de segurança implementado impede que chaves criptográficas assimétricas privadas sejam exportadas.

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

Procedimentos de ensaio para NSH 1 e 3.

EN.II.15.1: Analisar a documentação técnica e verificar se os métodos de sobrescrita de PCS empregados pelo módulo criptográfico apresentam suficiente proteção.

Procedimentos de ensaio para NSH 3.

EN.II.15.2: Por meio de análise do código fonte do software embarcado, verificar se os métodos de sobrescrita implementados estão em conformidade com a documentação fornecida, analisando a atomicidade dos mesmos.

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)".

Procedimentos de ensaio para NSH 1 e 3.

EN.II.16.1: Analisar a documentação técnica e verificar quais algoritmos criptográficos definidos na versão corrente do documento denominado "PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01)" são suportados pelo módulo criptográfico.

EN.II.16.2: Para cada um dos algoritmos criptográficos assimétricos suportados pelo módulo criptográfico e constantes no documento denominado "PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01)", realizar testes de validação baseados no modelo CAVP (*Cryptographic Algorithm Validation Program*) corrente do NIST. Os seguintes testes de validação para algoritmos criptográficos são aplicáveis:

- Testes de valores conhecidos KAT (*Known Answer Test*) disponibilizados pelo NIST.
- Cifração e decifração de valores conhecidos gerados pelo laboratório (seguir o mesmo padrão definido no CAVP).

EN.II.16.3: Para cada um dos algoritmos criptográficos simétricos suportados pelo módulo criptográfico e constantes no documento denominado "PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01)", realizar

testes de validação baseados no modelo CAVP (*Cryptographic Algorithm Validation Program*) corrente do NIST.

Os seguintes testes de validação para algoritmos criptográficos são aplicáveis:

- Testes de valores conhecidos KAT (*Known Answer Test*) disponibilizados pelo NIST.
- Cifração e decifração de valores conhecidos gerados pelo laboratório (seguir o mesmo padrão definido no CAVP).

Procedimentos de ensaio para NSH 3.

EN.II.16.4: Por meio de análise do código fonte do software embarcado, verificar se os algoritmos criptográficos suportados pelo módulo criptográfico e constantes no documento denominado "PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01)" foram implementados de acordo com seu respectivo padrão publicado pelo NIST (utilizar a versão corrente).

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.17.1: Analisar a documentação técnica e verificar como o módulo criptográfico impede que chaves criptográficas assimétricas privadas e chaves criptográficas simétricas de usuário, são impedidas de utilização antes da autenticação bem-sucedida do papel de acesso Usuário.

EN.II.17.2: Autenticar com sucesso no módulo criptográfico utilizando o papel de acesso Usuário. Logo após, com a chave assimétrica privada habilitada para uso, realizar operações criptográficas e verificar se tais operações foram concluídas com sucesso.

EN.II.17.3: Caso o módulo criptográfico suporte chave simétrica de usuário, autenticar com sucesso no módulo criptográfico utilizando o papel de acesso Usuário. Logo após, com a chave simétrica habilitada para uso, realizar operações criptográficas e verificar se tais operações foram concluídas com sucesso.

EN.II.17.4: Autenticar sem sucesso no módulo criptográfico utilizando o papel de acesso Usuário. Logo após, tentar realizar operações criptográficas com uma chave assimétrica privada armazenada no módulo criptográfico. Não deve ser possível a realização da referida operação criptográfica.

EN.II.17.5: Autenticar sem sucesso no módulo criptográfico utilizando o papel de acesso Usuário. Logo após, tentar realizar operações criptográficas com uma chave simétrica de usuário armazenada no módulo criptográfico. Não deve ser possível a realização da referida operação criptográfica.

Procedimentos de ensaio para NSH 3.

EN.II.17.6: Por meio de análise do código fonte do software embarcado, verificar como o módulo criptográfico impede que chaves criptográficas assimétricas privadas e chaves criptográficas simétricas de usuário, são impedidas de utilização antes da 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).

Procedimentos de ensaio para NSH 1 e 3.

EN.II.18.1: Analisar a documentação técnica e verificar os métodos de alteração de valor do PIN corrente disponibilizados pelo módulo criptográfico.

EN.II.18.2: Para cada um dos métodos de alteração do PIN corrente descritos na documentação técnica, realizar os referidos procedimentos verificando se o valor do PIN corrente foi alterado de forma assertiva à documentação.

EN.II.18.3: Caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança, verificar a possibilidade de alteração do PIN corrente por meio da inserção correta do PUK.

Procedimentos de ensaio para NSH 3.

EN.II.18.4: Por meio de análise do código fonte do software embarcado, verificar se os métodos utilizados para a alteração do PIN corrente estão em conformidade com os métodos apresentados na documentação técnica fornecida.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.19.1: Analisar a documentação técnica e verificar se os critérios utilizados pelo módulo criptográfico para a realização do bloqueio do PIN são suficientes.

EN.II.19.2: Seguindo os critérios para bloqueio do PIN descritos na documentação técnica, verificar se o módulo criptográfico bloqueia o PIN corrente após atingir o limite máximo de 5 tentativas de autenticação malsucedidas.

Procedimentos de ensaio para NSH 3.

EN.II.19.3: Por meio de análise do código fonte do software embarcado, verificar como o módulo criptográfico bloqueia o PIN corrente após atingir o limite máximo de 5 tentativas de autenticação 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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.20.1: Analisar a documentação técnica e verificar como o módulo criptográfico exerce a obrigatoriedade de troca do valor padrão do PIN de inicialização em seu primeiro acesso para o valor escolhido pelo proprietário do cartão criptográfico.

EN.II.20.2: Seguindo os procedimentos descritos na documentação técnica, verificar se no primeiro acesso ao módulo criptográfico o proprietário do cartão é informado sobre a obrigatoriedade de troca do valor padrão do PIN de inicialização. Após a realização da troca do valor padrão do PIN de inicialização, realizar operações criptográficas que validem a efetividade da troca do valor do PIN realizada.

Procedimentos de ensaio para NSH 3.

EN.II.20.3: Por meio de análise do código fonte do software embarcado, verificar como o módulo criptográfico obriga que no primeiro acesso ao mesmo o PIN padrão de inicialização seja alterado.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.21.1: Analisar a documentação técnica e verificar os procedimentos necessários para a reinicialização do módulo criptográfico, bem como, os métodos

utilizados para realizar a eliminação das chaves criptográficas de usuário e o valor do PIN corrente por meio da utilização do PUK.

EN.II.21.2: Reinicializar o módulo criptográfico de acordo com a documentação técnica fornecida e verificar se as chaves criptográficas pertencentes ao papel de acesso Usuário, bem como, o valor do PIN corrente, foram eliminados após o processo de reinicialização.

EN.II.21.3: Verificar se é possível a reutilização do módulo criptográfico após a reinicialização do mesmo.

Procedimentos de ensaio para NSH 3.

EN.II.21.4: Por meio de análise do código fonte do software embarcado, verificar se os procedimentos realizados para a reinicialização do módulo criptográfico bem como, os métodos utilizados para realizar a eliminação das chaves criptográficas de usuário e o valor do PIN corrente, estão em conformidade com os procedimentos apresentados na documentação técnica fornecida.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.22.1: Analisar a documentação técnica e verificar se a mesma descreve as formas de desbloqueio do papel de acesso Usuário após a inserção correta do PUK.

EN.II.22.2: Bloquear o PIN corrente e verificar se é possível o desbloqueio, mediante a inserção de um novo PIN, após informar corretamente o PUK. Após tal procedimento, verificar se o PIN corrente foi desbloqueado de forma bem-sucedida realizando alguma operação criptográfica.

Procedimentos de ensaio para NSH 3.

EN.II.22.3: Por meio de análise do código fonte do software embarcado, verificar se os procedimentos realizados para o desbloqueio do papel de acesso Usuário, estão em conformidade com os procedimentos apresentados na documentação técnica fornecida.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.23.1: Analisar a documentação técnica e verificar se esta descreve de forma suficiente a troca do PIN corrente, após autenticação bem-sucedida do usuário.

EN.II.23.2: Seguindo os procedimentos descritos na documentação técnica, trocar o PIN corrente após a autenticação bem-sucedida do usuário. Após tal procedimento, verificar se o PIN corrente foi trocado de forma bem-sucedida realizando alguma operação criptográfica.

Procedimentos de ensaio para NSH 3.

EN.II.23.3: Por meio de análise do código fonte do software embarcado, verificar se os procedimentos realizados para a troca do PIN corrente, estão em conformidade com os procedimentos apresentados na documentação técnica fornecida.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.24.1: Analisar a documentação técnica e verificar se os critérios de bloqueio do PUK apresentam suficiente proteção.

EN.II.24.2: Provocar o bloqueio do PUK no módulo criptográfico verificando se o procedimento realizado corresponde ao definido na documentação técnica.

Procedimentos de ensaio para NSH 3.

EN.II.24.3: Por meio de análise do código fonte do software embarcado, verificar se os procedimentos de bloqueio de PUK, estão em conformidade com os procedimentos apresentados na documentação técnica fornecida.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.25.1: Analisar a documentação técnica e verificar se os métodos de alteração do PUK apresentam suficiente proteção.

EN.II.25.2: Iniciar uma operação de troca do PUK verificando se o procedimento realizado corresponde ao definido na documentação técnica.

Procedimentos de ensaio para NSH 3.

EN.II.25.3: Por meio de análise do código fonte do software embarcado, verificar se os procedimentos de alteração do PUK, estão em conformidade com os procedimentos apresentados na documentação técnica fornecida.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.26.1: Analisar a documentação técnica e verificar se o mecanismo da não manutenção do código PUK em cache é suficiente.

EN.II.26.2: Por meio da técnica de dump de memória no equipamento de ensaio, verificar nos dados coletados se o código PUK permanece em cache.

Procedimentos de ensaio para NSH 3.

EN.II.26.3: Por meio de análise do código fonte do middleware, verificar se não há qualquer forma de armazenamento em cache do código PUK.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.27.1: Analisar a documentação técnica e avaliar a suficiência de proteção das situações nas quais o código PIN:

- É mantido em cache;
- Deve ser eliminado do cache.

EN.II.27.2: Realizar uma sequência de operações criptográficas que necessite do uso do PIN e verificar se, após a primeira operação criptográfica, o PIN não é mais solicitado, caraterizando a manutenção do código PIN em cache.

EN.II.27.3: Retirar o cartão criptográfico da leitora, inserir novamente e verificar se o módulo criptográfico realiza a solicitação do PIN antes da próxima operação criptográfica.

EN.II.27.4: Retirar o cartão criptográfico da leitora e por meio da técnica de dump de memória no equipamento de ensaio, verificar nos dados coletados se o código PIN é mantido em cache.

EN.II.27.5: Encerrar a aplicação corrente, iniciar novamente e verificar se o módulo criptográfico realiza a solicitação do PIN antes da próxima operação criptográfica.

EN.II.27.6: Encerrar a aplicação corrente e por meio da técnica de dump de memória no equipamento de ensaio, verificar nos dados coletados se o código PIN é mantido em cache.

EN.II.27.7: Caso seja possível configurar o tempo de duração máxima do PIN no cache (Time To Live – TTL), aguardar até que o tempo previamente configurado expire e verificar se o módulo criptográfico realiza a solicitação do PIN antes da próxima operação criptográfica.

EN.II.27.8: Caso seja possível configurar o tempo de duração máxima do PIN no cache (Time To Live – TTL), aguardar até que o tempo previamente configurado

expire e por meio da técnica de dump de memória no equipamento de ensaio, verificar nos dados coletados se o código PIN é mantido em cache.

EN.II.27.9: Analisar a documentação técnica e verificar se a mesma descreve quais os mecanismos de segurança adotados para proteger o PIN quando o mesmo é mantido em cache pela middleware.

EN.II.27.10: Realizar uma operação criptográfica que necessite como entrada o valor do PIN. Realizar uma segunda operação criptográfica para constatar que o PIN foi mantido em cache. Após a execução das referidas operações criptográficas, mantendo o módulo criptográfico energizado e a aplicação de testes em execução, utilizar a técnica de dump de memória no equipamento de ensaio e verificar nos dados coletados se o código PIN é mantido de forma protegida no cache de memória.

Procedimentos de ensaio para NSH 3.

EN.II.27.11: Por meio de análise do código fonte do middleware, verificar se os mecanismos de segurança adotados para a proteção do valor do código PIN em cache de memória foram implementados em conformidade com a documentação técnica fornecida.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.II.28.1: Analisar a documentação técnica e verificar se os métodos de eliminação do código PIN presentes no cache apresentam suficiente proteção.

Procedimentos de ensaio para NSH 3.

EN.II.28.2: Por meio de análise do código fonte do middleware, verificar os métodos utilizados para eliminar o código PIN do cache de memória.

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).

Procedimentos de ensaio para NSH 1 e 3.

EN.II.29.1: Analisar a documentação técnica e verificar se os controles de qualidade (caracteres alfanuméricos sensíveis a letras maiúsculas e minúsculas) e tamanho mínimo aplicados à definição dos códigos PIN e PUK (caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança) apresentam suficiente proteção**.**

EN.II.29.2: Tentar definir valores para PIN e/ou PUK (caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança) com tamanho inferior a 4 bytes. O módulo deve proibir a atribuição de valores de PIN e/ou PUK menores que 4 bytes.

EN.II.29.3: Definir valores para PIN e/ou PUK (caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança) com caracteres alfanuméricos maiúsculos e/ou minúsculos e tentar autenticar-se utilizando os mesmos caracteres, porém minúsculos, caso tenha sido definidos maiúsculos, e vice-versa. O módulo deve diferenciar os caracteres alfanuméricos maiúsculos dos respectivos caracteres minúsculos.

Procedimentos de ensaio para NSH 3.

EN.II.29.4: Por meio de análise do código fonte do middleware, verificar os métodos utilizados para garantir os controles de qualidade (caracteres alfanuméricos sensíveis a letras maiúsculas e minúsculas) e tamanho mínimo aplicados à definição dos códigos PIN e PUK (caso o módulo criptográfico suporte o papel de acesso Oficial de Segurança).

2.3. Requisitos de Interoperabilidade

2.3.1. Módulo criptográfico

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.

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.

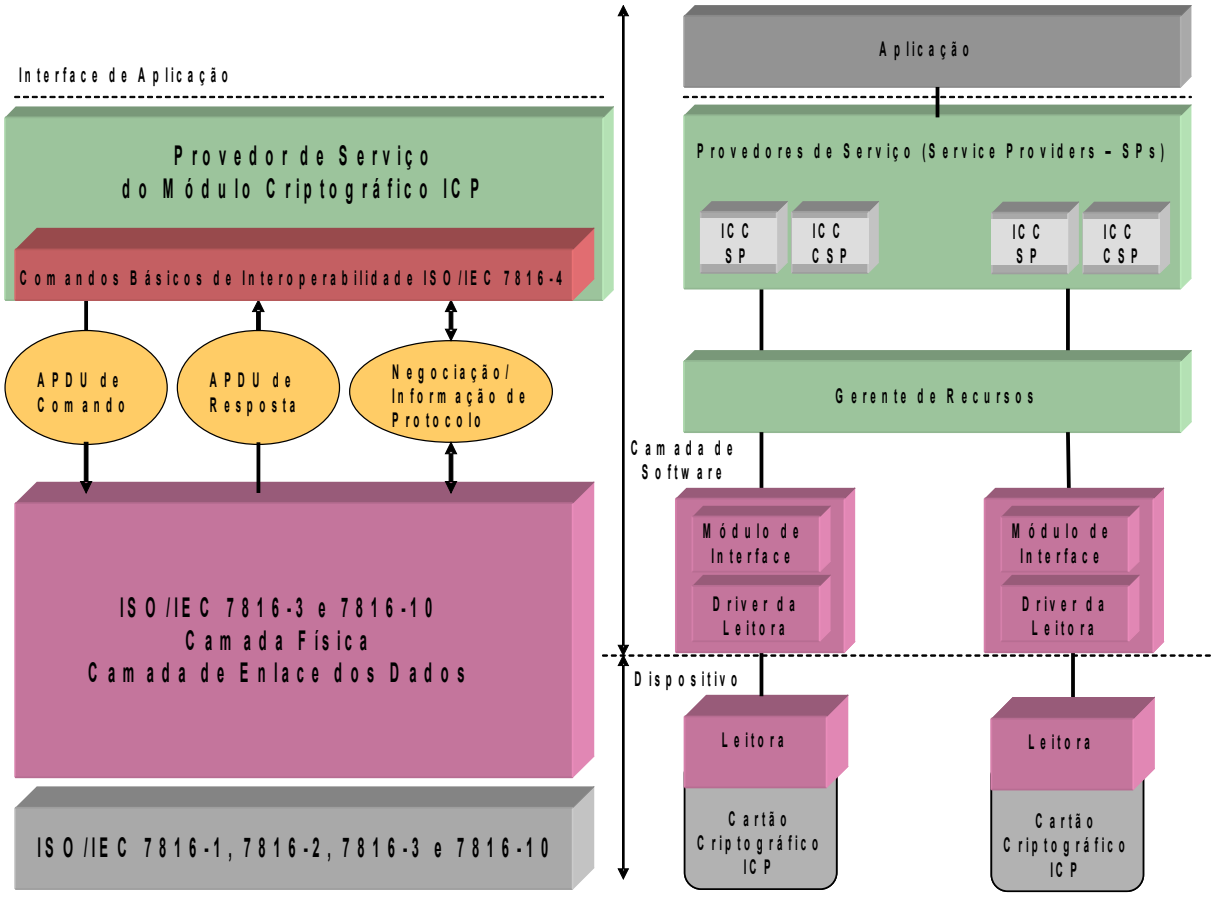

Figura 2. Arquitetura de interoperabilidade de cartões ISO 7816 e PC/SC

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, a codificação e as convenções definidas no padrão ISO/IEC 7816-4:2005.

Procedimentos de ensaio para NSH 1 e 3.

EN.III.1.1: Analisar a documentação técnica e verificar se a estrutura de comandos e respostas APDU estão em conformidade com a norma ISO/IEC 7816-4:2005.

EN.III.1.2: Por meio de ferramenta que executa comandos APDU, realizar testes para verificar se a estrutura de comandos e respostas APDU está aderente a norma ISO/IEC 7816-4:2005.

Procedimentos de ensaio para NSH 3.

EN.III.1.3: Por meio de análise do código fonte do software embarcado, verificar se a estrutura de comandos e respostas APDU está de acordo com a documentação.

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, em conformidade com as normas ISO/IEC 7816-4:2005, 7816-8:2004 e 7816-9:2004.

Comando	Instrução	Parte da ISO/IEC 7816	Seção
APPEND RECORD	E2	4	7.3.6
CHANGE REFERENCE DATA	24	4	7.5.7
CREATE FILE	E0	9	6.1
DELETE FILE	E4	9	6.2
EXTERNAL (/ MUTUAL) AUTHENTICATE	82	4	7.5.4
GENERATE ASYMMETRIC KEY PAIR	46	8	5.1
GET CHALLENGE	84	4	7.5.3
GET DATA	CA	4	7.4.2
GET RESPONSE	C0	4	7.6.1
MANAGE CHANNEL	70	4	7.1.2
MANAGE SECURITY ENVIRONMENT	22	4	7.5.11
PERFORM SECURITY OPERATION	2A	8	5.2
PUT DATA	DA	4	7.4.3
READ BINARY	B0	4	7.2.3
READ RECORD	B2	4	7.3.3
RESET RETRY COUNTER	2C	4	7.5.10
SELECT	A4	4	7.1.1
UPDATE BINARY	D6	4	7.2.5
UPDATE RECORD	DC	4	7.3.5
VERIFY	20	4	7.5.6

Tabela 3: Conjunto mínimo de comandos para módulos criptográficos

Procedimentos de ensaio para NSH 1 e 3.

EN.III.2.1: Analisar a documentação técnica e verificar seos comandos suportados pelo módulo criptográfico estão em conformidade com as normas ISO/IEC 7816-4:2005, 7816-8:2004 e 7816-9:2004.

EN.III.2.2: Por meio de ferramenta que executa comandos APDU, realizar testes para verificar se cada comando descrito na Tabela 2 é suportado pelo módulo criptográfico e se seus respectivos efeitos estão em conformidade com as normas ISO/IEC 7816-4:2005, 7816-8:2004 e 7816-9:2004.

Procedimentos de ensaio para NSH 3.

EN.III.2.3: Por meio de análise do código fonte do software embarcado, verificar se existem comandos APDU não declarados na documentação fornecida pela parte interessada. Caso existam, inspecionar o comportamento dos mesmos e verificar se estão de acordo com os requisitos deste MCT.

EN.III.2.4: Varrer o código fonte em busca de todos os comandos declarados na documentação, verificando se o formato corresponde ao descrito na documentação.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.III.3.1: Analisar a documentação técnica e verificar se os requisitos de ciclo de vida para um cartão criptográfico estão em conformidade com a norma 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.

Procedimentos de ensaio para NSH 1 e 3.

EN.III.4.1: Analisar a documentação técnica e verificar se os requisitos de gestão de aplicações para um cartão criptográfico multiaplicação estão em conformidade com a norma 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.

Procedimentos de ensaio para NSH 1 e 3.

EN.III.5.1: Analisar a documentação técnica e verificar se as dimensões do cartão criptográfico estão em conformidade com as normas ISO/IEC 7810:2003 e 7816-1:2003.

EN.III.5.2: Verificar no cartão criptográfico se as dimensões dos contatos presentes no cartão criptográfico estão em conformidade com a norma 7816-2:2003.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.III.6.1: Verificar se a documentação técnica especifica de forma suficiente como os contatos elétricos não usados são eletricamente isolados.

EN.III.6.2: Analisar se os contatos elétricos não usados estão eletricamente isolados entre si e em relação aos demais, medindo tal isolamento por meio de experimentação.

EN.III.6.3: Ativar o cartão criptográfico, colocando em modo de operação e verificar por meio de medida experimental a ausência de ligação elétrica com os contatos não usados.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.III.7.1: Analisar a documentação técnica e verificar se as interfaces elétricas e os protocolos de transmissão estão em conformidade com a norma ISO/IEC 7816-3:2006.

EN.III.7.2: Verificar no cartão criptográfico se as interfaces elétricas estão aderentes à norma ISO/IEC 7816-3:2006.

EN.III.7.3: Realizar testes para verificar se os protocolos de transmissão estão em conformidade com a documentação fornecida.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.III.8.1: Analisar a documentação técnica e verificar se o módulo criptográfico está aderente à família de padrões ISO/IEC 14443

EN.III.8.2: Realizar testes para verificar se o módulo criptográfico está aderente à 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.

Procedimentos de ensaio para NSH 1 e 3.

EN.IV.1.1: Verificar se a documentação técnica descreve a(s) API(s) e versão(ões) suportadas pelo módulo criptográfico.

EN.IV.1.2: Realizar teste para verificar a compatibilidade com a(s) versão(ões) da API(s) constantes na documentação técnica.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.IV.2.1: Analisar se a documentação técnica descreve de forma suficiente os requisitos funcionais de gerenciamento de chaves criptográficas.

EN.IV.2.2: Gerar chaves criptográficas assimétricas de forma aleatória no módulo criptográfico. Após a geração, verificar se a chave gerada está presente no módulo criptográfico e executar operações criptográficas que validem as chaves assimétricas.

EN.IV.2.3: Escolher uma determinada chave criptográfica assimétrica e depois recuperar seus parâmetros associados. Após a recuperação, verificar se os parâmetros obtidos correspondem à chave selecionada. Os parâmetros mínimos a serem recuperados são: algoritmo, tamanho da chave e permissões.

Procedimentos de ensaio para NSH 3.

EN.IV.2.4: Por meio de análise do código fonte do middleware, verificar os requisitos funcionais de gestão de chaves criptográficas.

EN.IV.2.5: Varrer o código fonte em busca de todos os comandos descritos na lista completa de comandos, verificando se o formato corresponde ao descrito na na documentação.

EN.IV.2.6: Varrer o código em busca de comandos não descritos. Caso existam, inspecionar o comportamento dos mesmos e verificar se estão de acordo com os requisitos deste MCT.

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.

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

Procedimentos de ensaio para NSH 1 e 3.

EN.IV.3.1: Analisar se a documentação técnica descreve de forma suficiente os requisitos de exportação e importação aplicáveis ao módulo criptográfico, bem como a middleware.

EN.IV.3.2: Importar cadeia de certificação para o módulo criptográfico. Após a importação verificar se a cadeia de certificação importada é válida e corresponde àquela selecionada durante a operação de importação.

EN.IV.3.3: Importar certificado digital para o módulo criptográfico segundo padrões X.509 versão 3. Após a importação, verificar se o certificado foi importado nos padrões requisitados e se tal certificado corresponde àquele selecionado durante a operação de importação.

EN.IV.3.4: Exportar chave criptográfica assimétrica pública do módulo criptográfico. Após a exportação, verificar se a chave foi exportada e executar operações criptográficas que validem a chave.

EN.IV.3.5: Exportar certificado digital de Usuário do módulo criptográfico. Após a exportação, verificar se o certificado foi exportado e se tal certificado corresponde àquele selecionado durante a operação de exportação.

EN.IV.3.6: Exportar cada um dos certificados da cadeia de certificação do módulo criptográfico. Após a exportação, verificar se cada um dos certificados da cadeia de certificação exportada é válida e corresponde àquela selecionada durante a operação de exportação.

EN.IV.3.7: Importar certificado de atributo para o módulo criptográfico segundo padrões X.509 versão 3. Após a importação, verificar se o certificado foi importado nos padrões requisitados e se tal certificado corresponde àquele selecionado durante a operação de importação.

EN.IV.3.8: Exportar certificado de atributo do módulo criptográfico. Após a exportação, verificar se o certificado foi exportado e se tal certificado corresponde àquele selecionado durante a operação de exportação.

Procedimentos de ensaio para NSH 3.

EN.IV.3.9: Por meio de análise do código fonte do middleware, verificar a implementação das funcionalidades de importação e exportação de chaves e certificados em questão, buscando verificar a inexistência de outras funcionalidades não declaradas.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.IV.4.1: Analisar a documentação técnica e verificar como a middleware assegura que as chaves simétricas, chaves assimétricas privadas e PCS sejam protegidas contra leitura, modificação, utilização e substituição não autorizada.

EN.IV.4.2: Tentar obter acesso às chaves simétricas, chaves assimétricas privadas e PCS para os quais não está autorizado, utilizando a API disponibilizada. O módulo

deve proibir que as chaves simétricas, chaves assimétricas privadas e PCS sejam visualizadas no formato de texto legível.

EN.IV.4.3: Tentar utilizar chaves simétricas e chaves assimétricas privadas para as quais não está autorizado, utilizando a API disponibilizada. O módulo deve proibir que as chaves simétricas e chaves assimétricas privadas sejam utilizadas sem o devido controle.

EN.IV.4.4: Tentar modificar ou substituir chaves simétricas, chaves assimétricas privadas e PCS para as quais não está autorizado, utilizando a API disponibilizada. O módulo deve proibir que as chaves simétricas, chaves assimétricas privadas e PCS sejam modificadas ou substituídas sem o devido controle.

Procedimentos de ensaio para o NSH 3.

EN.IV.4.5: Por meio de inspeção do código fonte da middleware, verificar como estes proíbem que as chaves simétricas e chaves assimétricas privadas sejam utilizadas sem a devida autorização.

EN.IV.4.6: Por meio de inspeção do código fonte da middleware, verificar como estes proíbem que as chaves simétricas, chaves assimétricas privadas e PCS sejam modificadas ou substituídas sem o devido controle.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.IV.5.1: Analisar a documentação técnica e verificar como a middleware assegura que as chaves assimétricas públicas sejam protegidas contra modificação e substituição não autorizada.

EN.IV.5.2: Tentar modificar ou substituir chaves assimétricas públicas para as quais não está autorizado, utilizando a API disponibilizada. O módulo deve proibir que as chaves assimétricas públicas sejam modificadas ou substituídas sem o devido controle.

Procedimentos de ensaio para NSH 3.

EN.IV.5.3: Por meio de inspeção do código fonte da middleware, verificar como estes proíbem que as chaves assimétricas públicas sejam modificadas ou substituídas sem o devido controle.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.IV.6.1: Analisar a documentação técnica e verificar como a middleware propaga os certificados digitais presentes no cartão criptográfico para o repositório do sistema operacional que pode ser lido por aplicações de usuários.

EN.IV.6.2: Inserir o cartão criptográfico numa leitora de cartões inteligentes compatível e verificar se os certificados digitais presentes no mesmo foram propagados para o repositório do sistema operacional que pode ser lido por aplicações de usuários de forma correta. Após a propagação, executar operações criptográficas que validem os certificados digitais propagados.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.V.1.1: Analisar a documentação técnica e verificar se as informações listadas a seguir encontram-se no idioma português do Brasil:

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

EN.V.1.2: Verificar se as versões dos componentes de software do produto fornecidos pela aplicação encontram-se compatíveis com a documentação técnica.

Procedimentos de ensaio para NSH 3.

EN.V.1.3: Analisar se o mecanismo de controle de integridade informado pela parte interessada garante a indissolubilidade entre o identificador e o código embarcado.

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.

Procedimentos de ensaio para NSH 1 e 3.

EN.V.2.1: Analisar a documentação técnica e verificar se foram tomadas as providências para evitar injeção de código arbitrário, *buffer overflow*, quebra de mecanismos de autenticação/controle de sessão e vazamento de memória.

Procedimentos de ensaio para NSH 3.

EN.V.2.2: Por meio de inspeção de código, verificar a inexistência de vulnerabilidades que permitam injeção de código arbitrário e quebra de mecanismos de autenticação/controle de sessão, e a inexistência de *buffer overflows* e vazamento de memória.

3. 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.

[FIPS PUB 201-2] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). **Federal Information Processing Standards Publication: Personal Identity Verification.** FIPS PUB 201-2. Washington. US Government Printing Office: August, 2013.

[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.

[NIST SP 800-76-2] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). ***Biometric Specification for Personal Identity Verification.*** Special Publication 800-76-2. July, 2013.

[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.