Infraestrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 7 – Volume II

Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP-Brasil

Versão 2.2

Brasília, 26 de setembro de 2017

SUMÁRIO

CONTROLE DE ALTERAÇÕES....4
SIGLAS E ACRÔNIMOS....5
LISTAS DE ILUSTRAÇÕES....7
1 INTRODUÇÃO....8
1.1 ORGANIZAÇÃO DESTE DOCUMENTO....8
2 PARTE 1....10
2.1.1 Requisitos de especificação do módulo criptográfico....11
2.1.1.1 Algoritmos criptográficos obrigatórios....20
2.1.2 Portas e interfaces do módulo criptográfico....24
2.1.3 Papéis, serviços e autenticação....29
2.1.3.1 Papéis de acesso....30
2.1.3.2 Papel de acesso Usuário....31
2.1.3.3 Papel de acesso Oficial de Segurança (SO)....32
2.1.3.4 Papel de acesso Manutenção....33
2.1.3.5 Serviços....34
2.1.3.6 Autenticação de operadores do módulo criptográfico....36
2.1.4 Modelo de estado finito....40
2.1.5 Segurança Física....43
2.1.5.1 Requisitos gerais de segurança física....43
2.1.5.2 Requisitos específicos para proteção que evidencia violação....45
2.1.5.3 Requisitos específicos de proteção que resiste à violação....47
2.1.5.4 Requisitos específicos de proteção que detecta e responde à violação....48
2.1.6 Ambiente operacional....49
2.1.6.1 Ambiente operacional não modificável....49
2.1.6.2 Ambiente operacional modificável....50
2.1.7 Gerenciamento de chaves criptográficas....53
2.1.8 Geradores de números aleatórios....55
2.1.9 Geração de chaves criptográficas....58
2.1.9.1 Requisitos específicos de geração de chaves criptográficas....59
2.1.9.2 Importação e exportação de chaves criptográficas....60
2.1.9.3 Requisitos específicos de exportação de chaves criptográficas....64

2.1.9.4 Atribuição de chaves....66
2.1.9.5 Armazenamento de chaves criptográficas....67
2.1.9.6 Sobrescrita do valor de chaves criptográficas com zeros binários....69
2.1.10 Interferência/compatibilidade eletromagnética....70
2.1.11 Auto-testes....71
2.1.11.1 Testes de energização....75
2.1.11.2 Testes condicionais....76
2.1.12 Garantia de projeto....81
2.1.13 Mitigações de ataques....84
2.2 Requisitos de gerenciamento....85
2.2.1.1 Backup e recuperação....85
2.2.1.2 Proteção contra falhas....85
2.2.1.3 Atualização e integridade do firmware....86
2.2.1.4 Controle de ativação com segredo compartilhado M de N (sistema Shamir Secret Sharing)....86
2.2.1.5 Utilitários de administração e diagnósticos....87
2.2.2 Gerenciamento do módulo criptográfico....87
2.2.3 Gerenciamento de chaves criptográficas....89
2.2.4 Exportação e importação....91
2.3 Requisitos de interoperabilidade....92
2.3.1 Requisitos gerais de interoperabilidade....92
2.3.1.1 Requisitos gerais....93
2.3.1.2 Requisitos sobre CryptoAPI....95
2.3.1.3 Requisitos sobre PKCS#11....97
2.3.1.4 Requisitos sobre Java Cryptographic Extension (JCE)....99
2.3.1.5 Requisitos sobre OpenSSL....102
2.3.2 Requisitos de armazenamento....103
2.4 Requisitos para restrição de substâncias nocivas....104
2.5 Requisitos de documentação....106
3 REFERÊNCIAS NORMATIVAS....109
ANEXO I....116

CONTROLE DE ALTERAÇÕES

Versão	Item Alterado	Descrição da Alteração
MCT 7 Vol. I Versão 2.2 IN 08, de 26/09/2017	2 e Anexo I	Previsão de autonomia para o OCP definir os ensaios nas Avaliações de Manutenção de Credenciamento.
MCT 7 Vol. II Versão 2.1	Índice	Numeração de itens para alinhar os volumes I e II
MCT 7 Vol. II Versão 2.0		Revisão do documento 08/11/2016
MCT 7 Vol. II Versão 1.0		Criação do Documento 26/11/2007

SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AES	*Advanced Encryption Standard*
API	*Application Programming Interface*
CBC	*Cipher Block Chaining*
CBC-MAC	*Cipher Block Chaining Message Authentication Code*
CMAC	*Cipher-based Message Authentication Code*
CMVP	*Cryptographic Module Validation Program*
CSP	*Cryptographic Service Provider*
DES	*Data Encryption Standard*
ECB	*Electronic Code Book*
FIPS	*Federal Information Processing Standards*
HMAC	*Keyed-Hash Message Authentication Cod*
HSM	*Hardware Security Module*
ICP	Infraestrutura de Chaves Públicas
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
JCA	*Java Cryptography Architecture*
JCE	*Java Cryptographic Extension*
CCM-MAC	Counter with CBC-MAC
MSC	Módulo de Segurança Criptográfico
NIST	*National Institute of Standards and Technology*
NSH	Níveis de Segurança de Homologação
PCS	Parâmetro Crítico de Segurança
PED	*PIN Entry Device*
PIN	*Personal Identification Number*
PKCS	*Public Key Cryptography Standards*
RNG	*Random Number Generators*
RSA	*Rivest, Shamir and Adleman*

SIGLA	DESCRIÇÃO
SDK	*Software Development Kits*
SHA	*Secure Hash Algorithm*
SO	Oficial de Segurança
SP	*Service Providers*
TDES	*Triple DES*
TRNG	*True Random Number Generator*

Listas de ilustrações

Lista de Figuras

Figura 1. Geradores de números aleatórios.....59

1 Introdução

Este documento descreve os procedimentos de ensaio para homologação de módulos de segurança criptográficos (MSC, também conhecidos como HSM – *Hardware Security Modules*) no âmbito da Infraestrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Os procedimentos de homologação fazem referência ao conjunto de métodos que serão usados para avaliar se um MSC está ou não em conformidade com os requisitos técnicos definidos pelo "Manual de Condutas Técnicas 7 - Volume I".

Ao final de cada requisito avaliado, devem ser descritos os resultados dos ensaios realizados e emitido um relatório, cuja conclusão deve indicar a aderência ao respectivo requisito.
Neste documento, o termo "módulo criptográfico" será usado em referência ao processador criptográfico interno do MSC.

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 por cento) do total dos requisitos previstos no Anexo I deste MCT para cada avaliação de manutenção no modelo 4 e de 33% (trinta e três por cento) 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.

1.1 Organização deste documento

Cada seção deste documento contém um conjunto de requisitos que representam citações diretas do próprio texto do "Manual de Condutas Técnicas 7 - Volume I". Os requisitos estão organizados da seguinte forma:

- "REQUISITO <número_do_requisito>.<número_de_sequência_do_requisito>"
    - "número_do_requisito": corresponde ao número de área definido no Manual de Condutas Técnicas 7 – Volume I;

- "número_de_sequência_do_requisito": corresponde a um identificador sequencial dos requisitos.

Os procedimentos de homologação visam a orientar sobre como proceder nos ensaios para um MSC. Os procedimentos de ensaio estão classificados e agrupados por Níveis de Segurança de Homologação da seguinte forma:

- NSH 1: Este nível não requer depósito e análise de código-fonte associado ao MSC em homologação;
- NSH 2: Este nível requer depósito e análise apenas de código-fonte de componentes específicos associados ao MSC em homologação. Por exemplo, código-fonte do algoritmo gerador de números aleatórios;
- NSH 3: Este nível requer depósito e análise de código-fonte completo associado ao MSC em homologação. Por exemplo, código-fonte de todo software do módulo criptográfico.

Os procedimentos de ensaio (EN) que devem ser desempenhados pelo analista LEA 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 sequencial dos procedimentos que devem ser desempenhados.

Os termos usados neste documento estão referenciados no MCT – Glossário Geral.

2 PARTE 1

2 Procedimentos de ensaio a serem observados no processo de homologação de Módulos de Segurança Criptográficos MSC

Requisitos Técnicos

Esta parte apresenta os procedimentos de ensaio que devem ser verificados no processo de homologação de MSC.

- Os procedimentos de ensaio descritos nesta parte englobam:
- Requisitos de especificação;
- Requisitos de segurança;
- Requisitos de interoperabilidade;
- Requisitos de gerenciamento;
- Requisitos funcionais;
- Requisitos de documentação.

2.1.1 Requisitos de especificação do módulo criptográfico

REQUISITO III.1.1: A parte interessada deve fornecer documentação específica dos componentes de hardware, software e *firmware* do módulo criptográfico além da fronteira criptográfica que delimita tais componentes.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.1.1.01: Verificar se a documentação inclui uma "lista de componentes principais" que descreve todos componentes de hardware, software e firmware do módulo criptográfico. Verificar se a "lista de componentes principais" inclui, mas não se limita aos seguintes tipos de componentes:

- Processadores, incluindo microprocessadores, processadores de sinal digital, processadores personalizados/dedicados, microcontroladores, ou quaisquer outros tipos de processadores;
- Circuitos integrados de memória ROM (*Read Only Memory*) para código executável de programas e dados [tal item pode incluir MPROM (*Mask-Programmed* ROM), PROM (*Programmable* ROM), EPROM (*Erasable* PROM), EEPROM (*Electrically Erasable* PROM) ou FLASH];
- Circuitos integrados de memória RAM (*Random Access Memory)* para armazenamento de dados temporários;

- Circuitos integrados semi dedicado (*semi-custom*) de aplicação específica, tais como, *gate arrays*, *programmable logic arrays*, *field programmable gate arrays*, ou outros dispositivos lógicos programáveis;
- Circuitos integrados totalmente dedicados (*fully custom*) e de aplicação específica, incluindo quaisquer circuitos integrados criptográficos e dedicados;
- Outros elementos ativos de circuito eletrônico (a documentação não deve listar elementos passivos de circuito eletrônico, tais como, resistores *pull up/pull down* ou capacitores *bypass* se eles não desempenharem um papel significativo na segurança do módulo criptográfico e não estiverem na fronteira criptográfica;
- Componentes de fornecimento de energia, incluindo alimentação (*power supply*), módulos de conversão de voltagem (por exemplo: módulos AC-DC ou DC-DC), transformadores, conectores de entrada de energia e conectores de saída de energia;
- Placa de circuito impresso ou outras superfícies de montagem de componentes;
- Encapsulamentos/revestimentos, incluindo quaisquer portas de acesso removíveis ou coberturas/camadas;
- Conectores físicos para dispositivos externos ao módulo criptográfico, ou entre quaisquer submódulos independentes do módulo principal;
- Módulos de software/*firmware* que são modificáveis;
- Módulos de software/*firmware* que não são modificáveis;
- Outros tipos de componentes que não estão listados acima.

EN.III.1.1.02: Verificar se a documentação especifica a fronteira criptográfica. A fronteira criptográfica deve incluir qualquer hardware ou software que insere, recebe, processa ou emite parâmetros de segurança importantes que poderiam conduzir ao comprometimento de informações sensíveis se não controlados adequadamente.

EN.III.1.1.03: Verificar se todos os componentes de hardware, software e *firmware* dentro da fronteira criptográfica estão incluídos na "lista de componentes principais", e se há componentes fora da fronteira criptográfica que não estão listados como componentes do módulo criptográfico.

EN.III.1.1.04: Verificar se a documentação mostra explicitamente e precisamente onde o perímetro físico da fronteira criptográfica está situado, incluindo detalhes sobre os seus componentes. Além disso, analisar se a documentação contém uma lista das portas conectadas aos equipamentos externos, todos os fluxos de informação significativa e processamentos a serem desempenhados dentro da fronteira criptográfica, além de toda informação recebida e emitida.

EN.III.1.1.05: Verificar se a fronteira criptográfica é fisicamente contínua, de tal forma que não haja lacunas que possam permitir entrada, saída ou outro tipo de acesso não controlado ao módulo criptográfico. O projeto do módulo criptográfico deve também assegurar que não tenham interfaces não controladas para o interior ou para fora do módulo criptográfico que possam passar PCSs *(*Parâmetros Críticos de Segurança*)*, dados em texto legível, ou outras informações que, se mal utilizadas ou utilizadas de forma inadequada, possam conduzir a um comprometimento da segurança.

EN.III.1.1.06: Verificar se todos os componentes que estão identificados no diagrama de blocos pertencem à fronteira criptográfica.

EN.III.1.1.07: Verificar se a documentação descreve os componentes de software/*firmware* executados pelo módulo criptográfico, bem como seus serviços desempenhados e os dispositivos de memória que armazenam dados e o código executável.

EN.III.1.1.08: Analisar a documentação e identificar os componentes de hardware internos ou externos ao módulo criptográfico que interagem com o processador listado na "lista de componentes principais".

REQUISITO III.1.2: A parte interessada deve fornecer documentação específica que descreve a configuração física do módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.1.2.01: Analisar a documentação e verificar se a identificação do módulo criptográfico está enquadrada numa das seguintes definições, conforme padrão FIPS PUB 140-2, Seção 4.5: *single-chip module*, *multi-chip embedded module* ou *multi-chip standalone module.*

EN.III.1.2.02: Analisar a documentação e verificar a disposição interna (*internal layout*) do módulo criptográfico por meio de desenhos técnicos, esboços ou diagramas de blocos que identifiquem cada bloco dos componentes de hardware.

EN.III.1.2.03: Analisar a documentação e verificar as principais montagens/encapsulamentos físicos do módulo e como são dispostas tais montagens/encapsulamentos no módulo criptográfico.

EN.III.1.2.04: Analisar a documentação e verificar a descrição dos parâmetros físicos principais do módulo criptográfico, constando, no mínimo, dos seguintes itens:

- Forma de encapsulamento/revestimento e dimensões aproximadas, incluindo quaisquer interfaces de acesso ou coberturas/camadas;
- Dimensões, disposição (*layout*) e interconexões de placa(s) de circuito impresso;
- Localização da fonte de alimentação de energia, conversores de energia e entradas e saídas de energia;
- Ativação de componentes interconectados por meio de condutores elétricos *(interconection wiring runs):* rotas e terminais;
- Arranjos de refrigeração, tais como, pratos de condução (*conduction plates)*, duto de refrigeração (*cooling airflow)*, trocadores de calor (*heat exchanger)*, haletas de refrigeração (*cooling fins)*, ventiladores (*fans)*, ou outros arranjos para a remoção de calor do módulo;
- Outros tipos de componentes não listados acima.

EN.III.1.2.05: Verificar se os itens descritos no EN.III.1.2.04 estão em conformidade com as estruturas físicas contidas na "lista de componentes principais".

REQUISITO III.1.3: A parte interessada deve fornecer documentação específica de qualquer componente de hardware, software ou *firmware* que seja excluído dos requisitos de segurança apresentados neste documento e explicar a razão para tal exclusão.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.1.3.01: Verificar se a documentação indica os componentes excluídos dos requisitos de segurança definidos no Manual de Condutas Técnicas 7 - Volume I.

EN.III.1.3.02: Analisar a documentação e identificar as razões e os argumentos apresentados pela PI para exclusão de componentes dos requisitos de segurança definidos no Manual de Condutas Técnicas 7 - Volume I. Verificar se as razões e argumentos apresentados para exclusão de componentes dos requisitos de segurança definidos no Manual de Condutas Técnicas 7 - Volume I são coerentes e precisos, não contendo pontos ambíguos e duvidosos.

EN.III.1.3.03: Verificar se a documentação mostra que um componente, se apresentar funcionamento inadequado, não pode causar comprometimento de PCSs, dados em texto legível, ou outras informações que se mal utilizadas ou utilizadas de forma inadequada poderiam conduzir a um comprometimento da segurança.

EN.III.1.3.04: Verificar se quaisquer interfaces ou conexões físicas entre os componentes excluídos e o módulo criptográfico, não permitem divulgação não controlada de PCSs, dados em texto legível, ou outras informações que se mal utilizadas ou utilizadas de forma inadequada poderiam conduzir a um comprometimento da segurança.

EN.III.1.3.05: Verificar se os componentes a serem excluídos dos requisitos do Manual de Condutas Técnicas 7 - Volume I estão também contidos na “lista de componentes principais”.

REQUISITO III.1.4: A parte interessada deve fornecer documentação específica de todas as portas físicas, interfaces lógicas e caminhos de dados definidos como de entrada e saída do módulo criptográfico.

Nota: Este requisito é testado como parte da **seção 3.2.**

REQUISITO III.1.5: A parte interessada deve fornecer documentação específica dos controles lógicos e manuais do módulo criptográfico.

Nota: Este requisito é testado como parte da **seção 3.2.**

REQUISITO III.1.6: A parte interessada deve fornecer documentação específica dos indicadores de estados lógicos e físicos do módulo criptográfico.

Nota: Este requisito é testado como parte da **seção 3.2.**

REQUISITO III.1.7: A parte interessada deve fornecer documentação específica das características elétricas, lógicas e físicas aplicáveis ao módulo criptográfico.

Nota: Este requisito é testado como parte da **seção 3.2.**

REQUISITO III.1.8: A parte interessada deve fornecer documentação específica que liste todas as funções de segurança e operações criptográficas que são empregadas pelo módulo, assim como especificar todos os modos de operação suportados, tanto os aprovados e os não-aprovados por um órgão homologador como o CMVP para FIPS 140. Essa documentação pode ser um manual do operador ou até uma política de segurança do FIPS 140-2 (vide FIPS 140-2 apêndice C) se o objeto de homologação previamente foi submetido para homologação no NIST.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.III.1.8.01: Verificar se a documentação fornecida descreve as funções de segurança (incluindo a lista de funções não aprovadas pela família de padrões FIPS), operações criptográficas e modos de operação suportados pelo módulo criptográfico.

REQUISITO III.1.9: A parte interessada deve fornecer documentação contendo um diagrama de blocos detalhando todos os principais componentes de hardware e de interconexão, incluindo:

- Microprocessadores;
- *Buffers* de entrada e saída;
- *Buffers* com conteúdo de texto claro;
- *Buffers* com conteúdo de texto cifrado;
- *Buffers* de controle;
- Memórias de armazenamento das chaves criptográficas;
- Memórias de armazenamento dos componentes de software do módulo, tornando explícito onde foram implementados o SO (Sistema Operacional) e os algoritmos criptográficos;
- Memória de trabalho ou operacional;
- Memória de programa;
- Componentes não listados acima.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.1.9.01: Verificar se a documentação contém um ou mais diagramas de blocos indicando os principais submódulos do módulo criptográfico. Neste caso, diagramas de blocos devem identificar, mas não estão limitados aos seguintes componentes:

- Microprocessadores ou quaisquer outros processadores presentes na "lista de componentes principais";
- *Buffer* (memória) que armazena dados de entrada ou saída considerados genéricos (exceto dados em texto plano e/ou cifrados ou informações de controle);
- *Buffer* (memória) de texto plano e/ou cifrado que armazena dados a serem cifrados ou decifrados;
- *Buffer* (memória) de controle que armazena informações de controle e estado que são inseridas ou retiradas do módulo criptográfico;
- Armazenamento de chaves criptográficas;
- Memória de trabalho ou operacional para processamento de informação;
- Memória de programa contendo o código executável de software ou *firmware*;
- Circuitos integrados (semi) dedicados (por exemplo, circuitos integrados de aplicação específica, *gate arrays, field programmable gate arrays, programmable logic arrays* ou outros dispositivos lógicos programáveis);

- Outros tipos de componentes não listados acima.

EN.III.1.9.02: Verificar se a documentação contém os diagramas de blocos que indicam os principais componentes de hardware, interconexões/interfaces internas e externas e fluxos de dados com componentes internos e externos ao módulo criptográfico.

EN.III.1.9.03: Verificar se os diagramas de blocos identificam o tipo de informação transmitida nas interconexões com componentes internos e externos ao módulo criptográfico.

EN.III.1.9.04: Verificar se os diagramas de blocos identificam os componentes pertencentes à fronteira criptográfica do módulo criptográfico.

REQUISITO III.1.10: A parte interessada deve fornecer documentação específica do projeto dos componentes de hardware, software e *firmware* do módulo criptográfico. Linguagens de especificação de alto nível para software e *firmware*, além de esquemas para hardware, devem ser usados para documentar o projeto. Essa documentação pode ser uma política de segurança não proprietária do FIPS 140-2 anexo C, se o objeto de homologação previamente foi submetido para homologação no NIST.
Essa documentação é obrigatória para o processo de homologação.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.1.10.01: Comparar a especificação do projeto de hardware, software e *firmware*, com a "lista de componentes principais" do módulo criptográfico.

EN.III.1.10.02: Verificar se há consistência entre o modelo de estado finito do módulo criptográfico e sua especificação de projeto.

EN.III.1.10.03: Verificar se a documentação do projeto foi realizada utilizando linguagens de especificação de alto nível para software e *firmware* e também esquemas para hardware.

REQUISITO III.1.11: A parte interessada deve fornecer documentação específica de todos os dados que são relacionados à segurança, demonstrando como e onde são armazenados tais dados nos componentes de hardware. Dados relacionados à segurança incluem, mas podem não estar limitados a:

- Chaves criptográficas secretas e privadas em texto claro e cifradas;
- Dados de autenticação, como por exemplo, senhas e PIN;
- PCS;
- Outras informações protegidas e de caráter sigiloso (por exemplo, dados de auditoria e eventos de auditoria), cuja divulgação ou modificação possa comprometer a segurança do módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.1.11.01: Verificar se a documentação atende ao **REQUISITO III.1.11.**

REQUISITO III.1.12: A parte interessada deve fornecer documentação específica da política de segurança adotada pelo módulo criptográfico. A política de segurança deve conter, de forma explicitamente indicada, as regras ou procedimentos que foram derivados dos requisitos definidos pelo padrão FIPS 140-2, assim como as regras ou procedimentos que foram derivados de quaisquer outros padrões ou requisitos adicionais impostos pelo fabricante (vide FIPS 140-2 anexo C).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.1.12.01: Examinar a política de segurança do módulo criptográfico e verificar se está em conformidade com os requisitos especificados no apêndice C do padrão FIPS PUB 140-2.

EN.III.1.12.02: Verificar se a documentação atende ao **REQUISITO III.1.12.**

2.1.1.1 Algoritmos criptográficos obrigatórios

Uma preocupação grande de um módulo criptográfico são os algoritmos criptográficos implementados. É importante que essas implementações estejam em conformidade com as normas e especificações respectivas.

REQUISITO III.1.13: O módulo criptográfico deve suportar no mínimo as seguintes funções criptográficas:

- Criptografia de dados:
  - DES (*Data Encryption Standard*) nos modos de operação ECB e CBC, apenas para uso legado (conforme padrão NIST FIPS PUB 46-3);
  - *Triple*-DES (3DES ou TDES) nos modos de operação ECB e CBC (conforme padrão NIST FIPS PUB 46-3);
  - AES (*Advanced Encryption Standard*) com tamanho de chave no mínimo 128 bits nos modos de operação ECB e CBC (conforme padrão NIST FIPS PUB 197);
- Autenticação de entidades com criptografia de chave pública:
  - RSA com tamanho mínimo de chaves de 2048 bits (conforme padrões ANSI X9.31 e PKCS#1 v. 1.5).
- Resumo criptográfico de dados (*Hash*):
  - SHA-1 (*Secure Hash Algorithm*), apenas para uso legado conforme padrão NIST FIPS PUB 180-2;
  - SHA-2 (*Secure Hash Algorithm*) conforme padrão NIST FIPS PUB 180-4.

Procedimentos de ensaio para NSH 1:

EN.III.1.13.01: Verificar se a documentação descreve os sistemas criptográficos suportados pelo módulo.

EN.III.1.13.02: Executar testes de criptografia de dados verificando o suporte pelo módulo criptográfico dos algoritmos DES e 3DES. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. Os documentos de testes de validação estão organizados para realizar testes automáticos em

componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de dados consistem em:

- Testes de respostas conhecidas (*Known Answer Tests*), que avaliam os componentes do DES e 3DES por meio dos parâmetros de entrada e de saída conhecidos. Estes testes também verificam a confiabilidade com relação aos erros de implementação nos componentes dos algoritmos;
- Testes de modo de operação (*Modes of Operation Tests*), que avaliam a possibilidade de haver erros feitos deliberadamente ou de forma maliciosa nas implementações dos algoritmos;
- Testes de mensagens de múltiplos blocos (*Multi-block message tests*), que avaliam os algoritmos no que se refere às mensagens com múltiplos blocos. Para o modo de operação CBC, verificar a exatidão das operações de cifragem/decifração destes algoritmos.

EN.III.1.13.03: Executar testes de criptografia de dados verificando o suporte pelo módulo criptográfico do algoritmo AES. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. Os documentos de testes de validação estão organizados para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de dados consistem em:

- Testes de respostas conhecidas (*Known Answer Tests*), que avaliam os componentes do AES por meio dos parâmetros de entrada e de saída conhecidos. Estes testes também verificam a confiabilidade com relação aos erros de implementação nos componentes dos algoritmos;
- Testes de modo de operação (*Modes of Operation Tests*), que avaliam a possibilidade de haver erros feitos deliberadamente ou de forma maliciosa nas implementações dos algoritmos;
- Testes de mensagens de múltiplos blocos (*Multi-block message tests*), que avaliam os algoritmos no que se refere às mensagens com múltiplos blocos. Para o modo de operação CBC, verificar a exatidão das operações de cifragem/decifração destes algoritmos.

EN.III.1.13.04: Executar testes de criptografia de chave pública verificando o suporte pelo módulo criptográfico do algoritmo RSA. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de chave pública consistem em:

- Teste de geração de assinaturas, que avalia a habilidade de uma IUT em gerar a assinatura correta que pode ser validada pela chave pública associada.
- Teste de verificação de assinaturas, que avalia a habilidade da IUT em reconhecer assinaturas válidas e inválidas;

Procedimentos de ensaio para NSH 2 e 3:

- Teste de geração de chaves, que avalia a habilidade em gerar os valores corretos dos componentes do algoritmo.

EN.III.1.13.05: Executar testes de resumo criptográfico de dados verificando o suporte pelo módulo criptográfico dos algoritmos SHA1, SHA256 e SHA512. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de resumo criptográfico de dados consistem em:

- Testes de mensagens curtas (*Short Message Test*), que avaliam a exatidão na geração do resumo criptográfico de dados com relação ao tamanho da mensagem de entrada;
- Testes de mensagens longas selecionadas (*Selected Long Message Test*), que avaliam a exatidão na geração do resumo criptográfico para mensagens que contêm múltiplos blocos;
- Testes de mensagens geradas pseudo-aleatoriamente (*Pseudorandomly generated messages test*), que verificam a exatidão dos resumos criptográficos de dados para mensagens geradas pseudo-aleatoriamente.

RECOMENDAÇÃO III.1.1: O módulo criptográfico também pode suportar a função DSA, conforme o padrão NIST FIPS PUB 186, para autenticação e assinatura digital de dados.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.1.1.01: Executar testes de autenticação e assinatura digital de dados verificando o suporte pelo módulo criptográfico do algoritmo DSA. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de chave pública consistem em:

- Teste de geração de chaves, que avalia a habilidade de uma IUT de gerar os valores corretos dos componentes do algoritmo;
- Teste de geração de assinaturas, que avalia a habilidade de uma IUT em gerar a assinatura correta que pode ser validada pela chave pública associada;
- Teste de verificação de assinaturas, que avalia a habilidade da IUT em reconhecer assinaturas válidas e inválidas.

RECOMENDAÇÃO III.1.2: De forma opcional, é sugerido que o módulo criptográfico também possa suportar as seguintes funções para autenticação e integridade:

- CBC-MAC baseado nos algoritmos 3DES ou AES, conforme padrão NIST PUB 800-38B;
- HMAC baseado nos algoritmos de resumos criptográficos implementados, conforme padrão NIST FIPS PUB 198;
- CMAC baseado nos algoritmos 3DES ou AES, conforme padrão NIST PUB 800-38B;
- MAC-CCM baseado no algoritmos 3DES ou AES, conforme padrão NIST PUB 800-38C).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.1.2.01: Verificar se a documentação descreve os algoritmos criptográficos suportados pela biblioteca criptográfica.

EN.REC.III.1.2.02: Executar testes de autenticação e integridade de dados verificando o suporte pela biblioteca criptográfica dos algoritmos CBC-MAC, HMAC, CMAC e MAC. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas. Os documentos de testes de validação estão organizados para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de autenticação de dados consistem em:

- Testes de respostas conhecidas (*Known Answer Tests*), que avaliam os componentes de CBC-MAC, HMAC, CMAC e MAC por meio dos parâmetros de entrada e de saída conhecidos. Estes testes também verificam a confiabilidade com relação aos erros de implementação nos componentes dos algoritmos;
- Testes de modo de operação (*Modes of Operation Tests*), que avaliam a possibilidade de haver erros feitos deliberadamente ou de forma maliciosa nas implementações dos algoritmos;
- *Testes de mensagens de múltiplos blocos (Multi-block message tests), que avaliam os algoritmos no que se refere às mensagens com múltiplos blocos.*

2.1.2 Portas e interfaces do módulo criptográfico

REQUISITO III.2.1: O fornecimento de energia elétrica (incluindo energia de uma fonte externa ou baterias) que entra no módulo criptográfico deve ser especificado na documentação do MSC. Uma entrada externa de energia não é necessária quando toda a energia é fornecida ou mantida internamente pelo módulo criptográfico (por ex. utilizando uma bateria interna).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.2.1.01: Verificar se a documentação especifica sobre o fornecimento de energia elétrica (incluindo energia de uma fonte externa ou baterias) que entra no módulo criptográfico.

REQUISITO III.2.2: Devem ser informadas todas as interfaces lógicas presentes no módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.2.2.01: Verificar se a documentação descreve as portas físicas e interfaces lógicas presentes no módulo criptográfico. Para cada interface lógica, é preciso verificar sua classificação quanto a:

- Interface de entrada de dados;
- Interface de saída de dados;
- Interface de entrada de controle;
- Interface de saída de estado.

EN.III.2.2.02: Analisar a documentação do módulo criptográfico e suas interfaces de entrada de dados, verificando que os seguintes tipos de dados podem ser inseridos e processados:

- Dados em texto claro que deve ser cifrado ou assinado pelo módulo criptográfico;
- Texto cifrado ou assinado que deve ser decifrado ou verificado pelo módulo criptográfico;
- Chaves criptográficas em texto claro ou cifradas e outros dados de gerenciamento de chaves que são inseridos e utilizados pelo módulo criptográfico, tais como, vetores e dados de iniciação, informação sobre particionamento de chaves, etc;
- Dados de autenticação em texto claro ou cifrado que devem ser inseridos no módulo criptográfico, tais como, senhas, PINs, e/ou informações biométricas;
- Informações de estado de fontes externas (por exemplo, outro módulo ou dispositivo criptográfico);
- Quaisquer outras informações que são inseridas no módulo criptográfico para processamento ou armazenamento, exceto informações de controle.

EN.III.2.2.03: Analisar a documentação do módulo criptográfico e suas interfaces de saída de dados, verificando que os seguintes tipos de dados podem ser emitidos:

- Dados em texto claro que foram decifrados pelo módulo criptográfico;
- Texto cifrado que foi criptografado pelo módulo;
- Assinaturas digitais que foram geradas pelo módulo criptográfico;
- Chaves criptográficas em texto claro ou cifradas e outros dados de gerenciamento de chaves que foram gerados internamente e emitidos pelo módulo criptográfico, tais como vetores e dados de iniciação, informação sobre particionamento de chaves, etc;

- Informações de controle emitidas pelo módulo criptográfico para entidades externas (por exemplo, outro módulo ou dispositivo criptográfico);
- Quaisquer outras informações que são emitidas pelo módulo criptográfico após processamento ou armazenamento, exceto informações de estado.

EN.III.2.2.04: Analisar a documentação do módulo criptográfico e suas interfaces de entrada de controle, verificando que todos os comandos, sinais e dados de controle (exceto dados inseridos via interface de entrada de dados) utilizados para controlar a operação do módulo criptográfico podem ser inseridos, tais como:

- Entradas de comandos lógicos via API, tais como, chamadas de função para uma biblioteca de software;
- Entradas de sinais de controle via uma ou mais portas físicas, tais como, comandos e sinais enviados por meio de porta serial;
- Entradas de controles manuais (por exemplo, usando chaves, botões ou um teclado);
- Quaisquer outros dados de controle.

EN.III.2.2.05: Analisar a documentação do módulo criptográfico e suas interfaces de saída de estado, verificando que todas informações de estado, sinais, indicadores lógicos e indicadores físicos utilizados para mostrar o estado do módulo criptográfico podem ser emitidos, tais como:

- Saídas lógicas de informações de estado via API, tais como, códigos de retorno de uma biblioteca de software;
- Saídas de sinais via uma ou mais portas físicas, tais como, informações de estado enviadas por meio de porta serial;
- Saídas manuais de estado (por exemplo, utilizando LEDs, alarme sonoro ou um display);
- Quaisquer outras informações de saída de estado.

REQUISITO III.2.3: O módulo criptográfico deve assegurar que o fluxo de informação e acesso físico sejam realizados pelas portas físicas e interfaces lógicas relacionadas.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.2.3.01: Analisar a documentação que descreve o fluxo de informação e acessos físicos ao módulo criptográfico, verificando que os seguintes aspectos são especificados:

- Todas portas de entradas e saídas físicas, incluindo as respectivas configurações de pinagens, localizações físicas dentro do módulo criptográfico, sumário dos sinais lógicos que passam através de cada porta e a sequência temporal de dois fluxos de sinais que compartilham o mesmo pino físico;
- Todas coberturas físicas, portas, aberturas, incluindo suas localizações físicas dentro do módulo criptográfico e os componentes ou funções que podem ser acessadas e/ou modificadas via cada cobertura/porta/abertura;
- Todas interfaces lógicas de entrada e saída, incluindo uma listagem ou diagrama de blocos que contêm as entradas (dados e/ou controles) e saídas (dados e/ou estados) do módulo criptográfico, juntamente com a descrição de tais interfaces;
- Todos elementos manuais utilizados para inserir fisicamente sinais de controle, tais como chaves ou botões, incluindo suas localizações físicas dentro do módulo criptográfico e uma listagem descrevendo os sinais de controle que podem ser inseridos manualmente;
- Todos os indicadores de estado físico, incluindo suas localizações físicas dentro do módulo criptográfico e uma listagem descrevendo os sinais de indicação de estado que são emitidos fisicamente;
- Um mapeamento das interfaces lógicas de entrada e saída para as portas de entrada e saída físicas, controles manuais e indicadores de estado físico do módulo criptográfico;
- Características físicas, lógicas e elétricas, quando aplicáveis, das portas e interfaces físicas citadas, incluindo um sumário dos sinais lógicos que passam por cada porta, níveis de tensão, seus significados lógicos e os tempos dos sinais.

EN.III.2.3.02: Verificar se a documentação especifica a relação dos fluxos de informações e pontos de acesso físico com as portas físicas e interfaces lógicas do módulo criptográfico, determinando que não há inconsistências com o Manual de Condutas Técnicas 7 - Volume I - seção 3.2, no que diz respeito a descrição dos componentes e configuração física das portas de entrada e saída.

EN.III.2.3.03: Verificar por inspeção direta se todas as especificações fornecidas na documentação estão consistentes com o projeto atual do módulo criptográfico.

REQUISITO III.2.4: Todo dado sendo inserido no módulo criptográfico via respectiva interface de entrada deve somente seguir pelo caminho de entrada definido. Da mesma forma, todo dado sendo emitido pelo módulo criptográfico via respectiva interface de saída deve somente seguir pelo caminho de saída definido.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.2.4.01: Verificar se a documentação fornecida descreve caminhos lógicos e físicos utilizados pelos dados entrantes no módulo criptográfico via interface de entrada. Verificar se os caminhos de entrada foram especificados com detalhamento suficiente para determinar por quais elementos os dados passam.

EN.III.2.4.02: Analisar se a documentação fornecida descreve os caminhos lógicos e físicos utilizados pelos dados que saem do módulo criptográfico via interface de saída. Verificar se os caminhos de saída foram especificados com detalhamento suficiente para determinar por quais elementos os dados passam.

Procedimentos de ensaio para NSH 2 e 3

EN.III.2.4.03: Analisar, por inspeção direta ao módulo criptográfico, se qualquer dado entrante via interface de entrada e portas físicas aplicáveis utiliza somente os caminhos especificados. Verificar se a especificação dos caminhos seguidos pelos dados entrantes é consistente com o projeto do módulo criptográfico.

EN.III.2.4.04: Analisar, por inspeção direta ao módulo criptográfico, se qualquer dado que sai via interface de saída e portas físicas aplicáveis utiliza somente os caminhos especificados. Verificar se a especificação dos caminhos seguidos pelos dados que saem é consistente com o projeto do módulo criptográfico.

REQUISITO III.2.5: Todo caminho de saída de dados deve ser logicamente desconectado dos circuitos e processos durante a geração, entrada ou destruição (preenchimento com zeros “0” binários) de chaves criptográficas.

Procedimentos de ensaio para NSH 1:

EN.III.2.5.01: Verificar se a documentação fornecida descreve como os caminhos utilizados pelos dados que saem do módulo criptográfico estão logicamente desconectados dos circuitos e processos que geram, apagam ou introduzem chaves criptográficas e PCSs.

EN.III.2.5.02: Verificar, por meio de analisador lógico e/ou osciloscópio, se nenhum dado está sendo liberado pelas interfaces e portas físicas associadas durante os processos que geram, apagam ou inserem chaves criptográficas.

Procedimentos de ensaio para NSH 2 e 3:

EN.III.2.5.03: Verificar, por análise direta ao código-fonte do módulo criptográfico, se os caminhos de saída de dados estão logicamente desconectados dos circuitos e processos que geram, apagam ou inserem chaves criptográficas, conforme documentação fornecida.

2.1.3 Papéis, serviços e autenticação

REQUISITO III.3.1: O módulo criptográfico deve suportar o conceito de "papel autorizado" para associação com operadores e serviços oferecidos pelo módulo.

Nota: Este requisito é testado como parte do **REQUISITO III.3.3**

REQUISITO III.3.2: O módulo criptográfico deve requisitar autenticação do operador quando do acesso ao módulo criptográfico. Assim, é possível para o módulo criptográfico verificar se o operador está autorizado a assumir o "papel" e, ainda, verificar se é permitido o acesso ao serviço requisitado neste papel assumido.

Nota: Este requisito é testado como parte do **REQUISITO III.3.3**

2.1.3.1 Papéis de acesso

REQUISITO III.3.3: [FIPS 140-2, 4.3.1] O módulo criptográfico deve suportar, no mínimo, os seguintes "papéis autorizados":

- **Oficial de segurança (SO)**: Necessário para realizar funções de gerenciamento, inicialização, distribuição e fechamento de acesso ao módulo.
- **Usuário**: Necessário para realização de serviços de segurança oferecidos pelo módulo depois de sua inicialização, incluindo operações criptográficas, criação de chaves criptográficas, o uso do sistema de arquivos, sobrescrita do valor de chaves criptográficas com zeros binários (*key zeroization*), etc;

- **Papel de Manutenção**: Necessário para realizar manutenção física e/ou manutenção lógica (por ex. diagnósticos de hardware/software) e auditoria. Todas as chaves secretas ou privadas armazenadas em texto claro assim como CSPs não protegidos devem ser "zerados" quando da entrada ou saída do papel de manutenção.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.3.01: Analisar a documentação referente a este requisito, verificando que, pelo menos, um papel de acesso "Usuário", um papel de acesso "Oficial de Segurança" e um papel de acesso "Manutenção" (se o módulo criptográfico permite a realização de serviços de manutenção física e/ou serviços de manutenção lógica) são definidos no módulo criptográfico, juntamente com seus serviços associados.

EN.III.3.3.02: Assumir no módulo criptográfico um papel de acesso "Usuário" e depois realizar testes executando serviços associados ao papel de acesso assumido, verificando se há ou não conformidade com a documentação fornecida.

EN.III.3.3.03: Assumir no módulo criptográfico um papel de acesso "Oficial de Segurança" e depois realizar testes executando serviços associados ao papel de acesso assumido, verificando se há ou não conformidade com a documentação fornecida.

EN.III.3.3.04: Assumir no módulo criptográfico um papel de acesso "Manutenção" e depois realizar testes executando serviços associados ao papel de acesso assumido, verificando se há ou não conformidade com a documentação fornecida.

REQUISITO III.3.4: [FIPS 140-2, 4.3.1] A documentação deve especificar todos os papéis autorizados que são suportados pelo módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.4.01: Verificar se a documentação atende ao **REQUISITO III.3.4.**

REQUISITO III.3.5: Para que o módulo criptográfico entre em operação, o operador deve ser autenticado, informando seu PIN correspondente, ou seja, o PIN do operador ou identidade por meio de *token* ou chave física.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.5.01: Verificar se a documentação descreve sobre o processo de autenticação do operador durante a inicialização do módulo criptográfico.

EN.III.3.5.02: Verificar se o operador é autenticado com a identidade por meio de *token* durante a inicialização do módulo criptográfico.

EN.III.3.5.03: Verificar se o operador é autenticado com uma chave física durante a inicialização do módulo criptográfico.

EN.III.3.5.04: Verificar se o operador é autenticado com a entrada de seu PIN correspondente durante a inicialização do módulo criptográfico.

2.1.3.2 Papel de acesso Usuário

REQUISITO III.3.6: Funcionalidades atribuídas ao papel de acesso "Usuário" devem incluir:

- Manipulação (leitura, escrita, criação e remoção) de chaves criptográficas e PCS no módulo criptográfico;
- Acesso às funcionalidades de segurança, como por exemplo: autenticação, transferência segura de mensagens por meios eletrônicos (*secure messaging*), criptografia, decifração, assinaturas digitais, geração de resumos criptográficos (*hashing*) e códigos MAC, etc;
- Geração de chaves RSA;
- Requisição de informações de estado do módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.6.01: Verificar se a documentação descreve as funcionalidades atribuídas ao papel de acesso "Usuário" descritas no **REQUISITO III.3.6**.

EN.III.3.6.02: Acessar o sistema como "Usuário" e verificar se este é capaz de:

- Manipular (leitura, escrita, criação e remoção) elementos no módulo criptográfico;
- Acessar as funcionalidades de segurança, como por exemplo: autenticação, transferência segura de mensagens por meios eletrônicos (*secure messaging*), criptografia, decifração, assinaturas digitais, geração de resumos criptográficos (*hashing*) e códigos MAC, etc;
- Gerar chaves RSA;
- Requisitar informações de estado do módulo criptográfico.

2.1.3.3 Papel de acesso Oficial de Segurança (SO)

REQUISITO III.3.7: Funcionalidades atribuídas ao papel de acesso "Oficial de Segurança" devem incluir:

- Inicialização do módulo criptográfico;
- Geração de chaves RSA;
- Sobrescrita do valor de chaves criptográficas com zeros "0" (*zeramento de chaves*);
- Finalização do módulo criptográfico;
- Execução de auto-testes;
- Requisição de informações de estado do módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.7.01: Verificar se a documentação descreve as funcionalidades atribuídas ao papel de acesso "Oficial de Segurança" descritas no **REQUISITO III.3.7**.

EN.III.3.7.02: Acessar o sistema como "Oficial de Segurança" e verificar se este é capaz de:

- Inicializar o módulo criptográfico;
- Gerar chaves RSA;
- Sobrescrever valor de chaves criptográficas com zeros "0" (*zeramento de chaves*);
- Finalizar o módulo criptográfico;
- Executar auto-testes;
- Requisitar informações de estado do módulo criptográfico.

2.1.3.4 Papel de acesso Manutenção

REQUISITO III.3.8: [FIPS 140-2, 4.3.1] Se o módulo criptográfico permite aos operadores realizar serviços de manutenção, o módulo deve suportar o seguinte papel de acesso autorizado:

- Papel de Manutenção: Esse papel é assumido para realizar manutenção física e/ou lógica como hardware e/ou software diagnósticos.

Procedimentos de ensaio para NSH 1, 2 e 3:
EN.III.3.8.01: Verificar se a documentação descreve sobre o módulo criptográfico dar permissão aos operadores realizar serviços de manutenção.

EN.III.3.8.02: Verificar se a documentação descreve sobre o papel de acesso autorizado "Manutenção".

EN.III.3.8.03: Acessar o sistema como papel de "Manutenção" e verificar se este é capaz de realizar manutenção física e/ou lógica como hardware e/ou software diagnósticos.

REQUISITO III.3.9: [FIPS 140-2, 4.3.1] A documentação do módulo criptográfico deve especificar completamente o papel de acesso de manutenção por nome e serviços permitidos.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.9.01: Verificar se a documentação especifica completamente o papel de acesso de manutenção por nome e serviços permitidos.

REQUISITO III.3.10: Funcionalidades atribuídas ao papel de acesso "Manutenção" devem incluir:

1. *Backup* de chaves
2. Recuperação de chaves
3. Configuração de operadores
4. Configuração e controle de logs

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.10.01: Verificar se a documentação descreve as funcionalidades atribuídas ao papel de acesso "Manutenção" descritas no **REQUISITO III.3.10**.

EN.III.3.10.02: Acessar o sistema como "Manutenção" e verificar se este é capaz de:

- Fazer *Backup* de chaves;
- Recuperar chaves;
- Configurar operadores;
- Configurar e controlar logs.

2.1.3.5 Serviços

REQUISITO III.3.11: [FIPS 140-2, 4.3.2] O módulo criptográfico deve prover os seguintes serviços aos operadores:

- "Mostrar estado": resultado do estado corrente do módulo;
- "Realizar auto-teste": executar auto-testes especificados na documentação do módulo criptográfico;

- "Realizar função de segurança aprovada": Realizar no mínimo uma operação de uma função de segurança aprovada num modo de operação aprovado. Por exemplo, utilizando o algoritmo de chaves simétricas AES no modo de operação CBC.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.11.01: Verificar se a documentação descreve os serviços oferecidos pelo módulo criptográfico aos operadores.

EN.III.3.11.02: Verificar se os serviços "Mostrar estado", "Realizar auto-teste" e "Realizar função de segurança aprovada" precisam estar associados a um papel de acesso.

EN.III.3.11.03: Executar o serviço "Mostrar estado" e verificar se está em conformidade com a documentação.
EN.III.3.11.04: Executar o serviço "Realizar auto-teste" e verificar se está em conformidade com a documentação (este ensaio deve ser realizado em conjunto com a seção 3.9 deste documento).

EN.III.3.11.05: Executar o serviço "Realizar função de segurança aprovada" e verificar se está em conformidade com a documentação.

REQUISITO III.3.12: [FIPS 140-2, 4.3.2] A documentação do módulo criptográfico deve especificar:

- Os serviços oferecidos pelo módulo como, por exemplo, serviços criptográficos;
- para cada serviço oferecido pelo módulo, suas "entradas de serviço", suas correspondentes "saídas de serviço" e os papéis de acesso autorizados nos quais o serviço pode ser realizado;
- qualquer serviço fornecido pelo módulo criptográfico para o qual um operador não necessita assumir um papel autorizado. Considerando estes serviços, deve-se mostrar que não afetam a segurança do módulo e, ainda, não modificam, divulgam ou substituem chaves criptográficas e PCS.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.12.01: Verificar se a documentação atende ao **REQUISITO III.3.12.**

2.1.3.6 Autenticação de operadores do módulo criptográfico

REQUISITO III.3.13: [FIPS 140-2 nível 2, 4.3.3] O módulo criptográfico deve empregar o mecanismo de autenticação baseado em papel de acesso para controlar o acesso ao módulo criptográfico.

Nota: Este requisito é testado como parte do **REQUISITO III.3.3.**

REQUISITO III.3.14: [FIPS 140-2, 4.3.3] Quando o módulo criptográfico for desligado e na sequência ligado novamente, os resultados de autenticações prévias não devem ser retidos e o módulo deve requisitar que o operador seja novamente autenticado.
Vários tipos de dados de autenticação podem ser requisitados pelo módulo criptográfico para implementar os mecanismos de autenticação suportados, incluindo, mas não limitado a:

1. Conhecimento ou posse de uma senha, PIN, chave criptográfica ou equivalente;
2. Posse de uma chave física, *token* ou equivalente.

Procedimentos de ensaio para NSH 1, 2 e 3:
EN.III.3.14.01: Verificar se a documentação descreve os mecanismos e os critérios usados pelo módulo criptográfico para eliminar os resultados de autenticações prévias.

EN.III.3.14.02: Autenticar-se nos papéis suportados no módulo e executar serviços associados. Em seguida, energizar e desenergizar o módulo e tentar executar alguns serviços dos papéis assumidos anteriormente.

EN.III.3.14.03: Verificar se o módulo nega o acesso aos serviços e requer nova autenticação.

EN.III.3.14.04: Baseando-se nos **EN.III.3.14.02** e **EN.III.3.14.03**, verificar se há conformidade com o **REQUISITO III.3.14**.

REQUISITO III.3.15: [FIPS 140-2, 4.3.3] Dados de autenticação armazenados no interior do módulo criptográfico devem ser protegidos contra divulgação, modificação e substituição não autorizada.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.15.01: Verificar se a documentação descreve como dados de autenticação armazenados no interior do módulo criptográfico são protegidos contra divulgação, modificação e substituição não autorizada.
EN.III.3.15.02: Tentar obter acesso aos dados de autenticação para os quais não está autorizado, usando métodos específicos. O módulo deve negar o acesso ou permitir somente o acesso aos dados cifrados ou protegidos de alguma forma.

EN.III.3.15.03: Tentar modificar ou substituir dados de autenticação para os quais não está autorizado, usando métodos específicos. Verificar se o módulo não permite que dados de autenticação sejam modificados ou substituídos.

REQUISITO III.3.16: [FIPS 140-2, 4.3.3] A força ou robustez do mecanismo de autenticação deve estar em conformidade com as seguintes especificações:

- Para cada tentativa de uso do mecanismo de autenticação, a probabilidade deve ser menor do que 1 em 1.000.000, de que uma tentativa aleatória tenha sucesso ou que uma aceitação falsa possa ocorrer (por exemplo, adivinhação de senha ou PIN, taxa de erro de aceitação falsa de um dispositivo biométrico ou alguma combinação de métodos de autenticação);
- para tentativas múltiplas de uso do mecanismo de autenticação durante um período de um minuto, a probabilidade deve ser menor do que 1 em 1.000.000, de que uma tentativa aleatória tenha sucesso ou que uma aceitação falsa possa ocorrer;
- a realimentação de dados de autenticação (*echo*) para um operador deve ser obscura durante a autenticação (por exemplo, nenhuma exibição visível de caracteres deve haver no momento da inserção de uma senha);

- a realimentação de dados de autenticação (*echo*) fornecida a um operador durante uma tentativa de autenticação, não deve enfraquecer a robustez do mecanismo de autenticação.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.16.01: Analisar a documentação, verificando, para cada mecanismo de autenticação suportado, que a probabilidade de uma tentativa aleatória ter sucesso ou de que uma aceitação falsa possa ocorrer, seja menor que 1 em 1.000.000.

EN.III.3.16.02: Para cada mecanismo de autenticação suportado, deve-se determinar o nível de exatidão de qualquer argumento fornecido via descrição analítica, verificando a existência de incertezas, pontos obscuros ou ambiguidades que possam comprometer o entendimento da documentação.

EN.III.3.16.03: Verificar por análise direta, se o dado de autenticação é obscurecido e se não há retorno visível durante a sua entrada.

EN.III.3.16.04: Verificar por análise direta, se mecanismo de realimentação não provê informações que poderiam ser usadas para adivinhar ou determinar os dados de autenticação.

EN.III.3.16.05: Realizar os ensaios **EN.III.3.16.03** e **EN.III.3.16.04** para cada papel suportado pelo módulo criptográfico.

REQUISITO III.3.17: [FIPS 140-2, 4.3.3] A documentação do módulo criptográfico deve especificar:

- Os mecanismos de autenticação suportados pelo módulo criptográfico;
- Os tipos de dados de autenticação que são requisitados pelo módulo para implementar os mecanismos de autenticação suportados;
- Os métodos autorizados que são utilizados para realizar o controle de acesso ao módulo criptográfico no seu primeiro acesso e, em seguida, inicializar o mecanismo de autenticação;

- A força e robustez dos mecanismos de autenticação suportados pelo módulo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.17.01: Verificar se a documentação atende ao **REQUISITO III.3.17.**

REQUISITO III.3.18: [FIPS 140-2, 4.3.3] Controle de acesso

- Para nível de segurança 1 e 2, o módulo criptográfico deve requerer autenticação baseado em papéis para controlar o acesso ao módulo.
- Para nível de segurança 3, o módulo criptográfico deve requerer autenticação baseado em identidades para controlar o acesso ao módulo.

Nota: Este requisito é testado como parte do **REQUISITO III.3.3 e REQUISITO III.3.5.**

REQUISITO III.3.20: [FIPS 140-2, 4.3.3] Caso o módulo utilize dispositivos de hardware no processo de autenticação, a documentação do módulo criptográfico deve especificar:

- Os tipos de hardware utilizados como:
  - Hardware *Tokens;*
  - *Token Reader;*
  - *PIN Entry Device (PED);*
  - *Operator Smart Cards;*
  - *Smartcard Reader;*
  - etc.
- A configuração do hardware para o processo de autenticação
  - *PIN Entry Device Keys;*
  - etc.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.3.20.01: Verificar se a documentação atende ao **REQUISITO III.3.20.**

2.1.4 Modelo de estado finito

REQUISITO III.4.1: [FIPS 140-2, 4.4] O diagrama de transição de estados e/ou a tabela de transição de estados deve incluir:

a) Todos os estados operacionais e estados de erro do módulo criptográfico;
b) As transições de um estado ao outro;
c) Os eventos de entrada que causam transições de um estado para outro;
d) Os eventos de saída resultantes das transições de um estado para outro.

Nota: Este requisito é testado como parte do **REQUISITO III.4.4.**

REQUISITO III.4.2: [FIPS 140-2, 4.4] O módulo criptográfico deve incluir os seguintes estados operacionais e estados de erro:

a) Estados de alimentação de energia: Estados para alimentação de energia primária, secundária ou *backup*. Estes estados podem se diferenciar em função das fontes de energia que estão sendo aplicadas ao módulo criptográfico;
b) Estados do "Oficial de Segurança": Estados nos quais os serviços do oficial de segurança (SO) são realizados (por exemplo, inicialização e gerenciamento de chaves criptográficas);
c) Estados "Entrada de chave ou PCS": Estados para a inserção de chaves criptográficas e PCS no módulo criptográfico;
d) Estados de usuário: Estados nos quais os usuários autorizados obtêm serviços de segurança, realizam operações criptográficas ou desempenham outras funções;
e) Estados de auto-teste: Estados nos quais o módulo criptográfico realiza auto-testes;
f) Estados de erro: Estados quando o módulo criptográfico encontra um erro (por exemplo, falha em um auto-teste ou tentativa de criptografar quando chaves operacionais ou PCS foram perdidos). Estados de erro poderiam incluir: a) "Erros críticos", os quais indicam um mal funcionamento do equipamento, podendo ser necessário executar serviços de manutenção ou reparo no módulo criptográfico; b) "Erros leves e recuperáveis", os quais requerem apenas uma nova inicialização (*resetting*) do módulo criptográfico. A recuperação a partir de estados de erro deve ser possível, exceto para os casos em que ocorram os "Erros críticos".

Nota: Este requisito é testado como parte do **REQUISITO III.4.4.**

REQUISITO III.4.3: Não é aceito qualquer tipo de estados de desvio (*bypass*) na homologação de equipamentos MSC no âmbito ICP-Brasil conforme descrito na observação a cima.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.4.3.01: Verificar se a documentação atende ao **REQUISITO III.4.3.**

EN.III.4.3.02: Executar testes que permitam afirmar que não há nenhum desvio na homologação do módulo criptográfico.

REQUISITO III.4.4: [FIPS 140-2, 4.4] A documentação do módulo criptográfico deve incluir uma representação do modelo de estado finito (ou equivalente), utilizando um diagrama de transição de estados e/ou uma tabela de transição de estados que deve especificar:

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

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.4.4.01: Analisar a documentação e verificar se contém uma descrição do modelo de estado finito. Esta descrição deve conter a identificação e detalhamento de todos os estados do módulo e as respectivas transições de estados. A descrição das transições de estados deve incluir condições internas do módulo, entradas de dados e controles que causam transições de um estado para outro e saídas de dados e estados resultantes das transições de um estado para outro.

EN.III.4.4.02: Verificar se os diagramas de estado finito e as respectivas descrições estão consistentes com a documentação, no que diz respeito aos seguintes ítens:

- Interface de entrada de dados;
- Interface de saída de dados;
- Interface de entrada de controle;
- Interface de saída de estado;
- Papel do oficial de segurança;
- Papel do usuário;
- Outros papéis (se aplicável);
- Entrada de chaves (se aplicável);
- Mostrar estado do serviço;
- Auto-teste;
- Outros serviços autorizados, operações e funções (se aplicável);
- Estados de erro;
- Estados de contorno (se aplicável);
- Interface de manutenção (se aplicável);
- Papel de manutenção (se aplicável);
- Serviço de geração de chave (se aplicável);
- Serviço de exportação de chave (se aplicável);
- Estado de ociosidade (se aplicável);
- Estado de não iniciação (se aplicável).

EN.III.4.4.03: Verificar se todo estado identificado no diagrama de estado finito possui a respectiva identificação e descrição na documentação e vice-versa.

EN.III.4.4.04: Verificar se a operação do módulo criptográfico está consistente com a descrição do diagrama de estado finito.

EN.III.4.4.05: Verificar, quando aplicável, se todos os estados de manutenção estão contidos no diagrama de estado finito.

EN.III.4.4.06: Verificar se existe uma cadeia de transições de um estado inicial de energização (*initial power-on state*) para cada estado no modelo, exceto para o próprio estado inicial de energização.

EN.III.4.4.07: Verificar se existe uma cadeia de transições de cada estado ativo do modelo para o estado de desativação (*power-off state*).

EN.III.4.4.08: Analisar a documentação e verificar se as ações do modelo de estado finito, como resultado de todas as possíveis entradas de dados e controles, estão bem definidas.

EN.III.4.4.09: Verificar se o módulo criptográfico suporta os seguintes estados operacionais e estados de erro:

- Estados de alimentação de energia;
- Estados do "Oficial de Segurança";
- Estados de "Entrada de chave ou PCS";
- Estados de usuário;
- Estados de auto-teste.

2.1.5 Segurança Física

2.1.5.1 Requisitos gerais de segurança física

REQUISITO III.5.1: A documentação técnica do módulo criptográfico deve especificar todos os componentes de hardware, software, *firmware* que estão contidos dentro da fronteira criptográfica e protegidos pelos mecanismos de segurança física.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.1.01: Analisar a documentação e verificar se a documentação atende ao **REQUISITO III.5.1.**

REQUISITO III.5.2: A documentação técnica do módulo criptográfico deve especificar quais mecanismos de segurança física estão implementados no módulo e seus respectivos componentes.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.2.01: Analisar a documentação e verificar se a documentação atende ao **REQUISITO III.5.2.**

REQUISITO III.5.3: A documentação técnica do módulo criptográfico deve descrever as interfaces de acesso para manutenção e os mecanismos de destruição de chaves criptográficas simétricas e assimétricas privadas e PCSs que são ativados quando a interface de acesso para manutenção for utilizada.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.3.01: Analisar a documentação e verificar se a documentação atende ao **REQUISITO III.5.3.**

REQUISITO III.5.4: Portas, tampas ou interfaces de acesso para manutenção, quando presentes no módulo criptográfico, devem ser protegidas com sensores que detectam o acesso a estas portas. A ativação de tais sensores deve iniciar instantaneamente no módulo criptográfico um processo de destruição de informações críticas armazenadas em sua memória, como por exemplo, chaves criptográficas ou parâmetros críticos de segurança.
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.4.01: Verificar se a documentação técnica descreve os sensores que detectam o acesso às portas, tampas ou interfaces de acesso para manutenção do módulo criptográfico.

EN.III.5.4.02: Verificar se a documentação técnica descreve os processos de destruição de informações críticas armazenadas na memória do módulo criptográfico na presença de acesso às interfaces de manutenção.

EN.III.5.4.03: Verificar por meio de inspeção direta no módulo criptográfico se portas, tampas ou interfaces de acesso para manutenção estão protegidas com sensores que detectam o acesso a estas portas.

EN.III.5.4.04: Provocar por meio de acesso direto às interfaces de manutenção a ativação dos sensores instalados nestas interfaces. Após o acesso realizado às interfaces de manutenção, verificar se todas as informações críticas armazenadas na memória do módulo foram destruídas.

REQUISITO III.5.5: Se o módulo criptográfico possuir orifícios ou fendas para ventilação, então estas devem ser construídas de forma a prevenir qualquer tipo de sondagem ou observação indevida do interior do módulo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.5.01: Verificar se a documentação técnica descreve as características físicas de orifícios ou fendas para ventilação presentes no módulo criptográfico.

EN.III.5.5.02: Verificar por meio de inspeção direta no módulo criptográfico, se orifícios ou fendas para ventilação estão dispostos e construídos de forma a prevenir a sondagem ou observação indevida do interior do módulo criptográfico.

2.1.5.2 Requisitos específicos para proteção que evidencia violação

REQUISITO III.5.6: Os componentes do módulo criptográfico devem ser envolvidos por uma cobertura ou camada que evidencie tentativas de acesso físico ao módulo. Esta cobertura ou camada que evidencia violações possui o intuito de deter a observação, sondagem ou manipulação direta do módulo, e portanto, provendo evidências de tentativa de violar ou remover componentes do módulo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.6.01: Verificar se a documentação técnica descreve o(s) material(is) delimitador(es) do módulo criptográfico e a finalidade a(s) qual(is) ele(s) se destina(m).

EN.III.5.6.02: Inspecionar o módulo criptográfico por meio de equipamentos específicos e caracterizar fisicamente a cobertura/camada que reveste o módulo criptográfico.

EN.III.5.6.03: Realizar tentativas de penetração física no módulo criptográfico por meio de técnicas específicas, de forma a causar o mínimo possível de evidência de violação na cobertura/camada que reveste o módulo criptográfico. Após tentativas de penetração no módulo criptográfico verificar se a cobertura/camada que reveste o módulo criptográfico produziu evidências suficientes para comprovar que houve tentativa de violação.

REQUISITO III.5.7: A cobertura ou camada que evidencia violações dos componentes do módulo criptográfico deve ser rígida e opaca ao espectro de luz visível.
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.7.01: Verificar se a documentação técnica descreve a opacidade e rigidez da(s) cobertura(s)/camada(s) que evidenciam violações do módulo criptográfico.

EN.III.5.7.02: Inspecionar o módulo criptográfico por meio de equipamentos específicos e caracterizar a opacidade da cobertura/camada que evidencia violações físicas.

EN.III.5.7.03: Realizar tentativas de sondagem ou observação no módulo criptográfico por meio de técnicas específicas e verificar se qualquer informação pode ser obtida a respeito do módulo.
REQUISITO III.5.8: Quando o módulo criptográfico possuir portas ou coberturas removíveis, estas deverão ser fechadas com cadeados ou fechaduras resistentes às violações que empregam chaves físicas ou lógicas protegidas por lacres que evidenciam violações.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.8.01: Verificar se a documentação técnica descreve a segurança contra violações de portas ou coberturas removíveis presentes no módulo criptográfico.

EN.III.5.8.02: Quando aplicável, inspecionar e caracterizar portas ou coberturas removíveis presentes no módulo criptográfico por meio de equipamentos específicos e verificar se estão protegidas com cadeados ou fechaduras resistentes à violação ou por lacres que evidenciam violações.

EN.III.5.8.03: Quando aplicável, inspecionar e caracterizar cadeados e fechaduras presentes no módulo criptográfico por meio de equipamentos específicos e verificar se tais itens são resistentes à violação.

EN.III.5.8.04: Quando aplicável, inspecionar e caracterizar lacres presentes no módulo criptográfico por meio de equipamentos específicos e verificar se tais itens evidenciam violação.

2.1.5.3 Requisitos específicos de proteção que resiste à violação

REQUISITO III.5.9: Os principais componentes do módulo criptográfico devem ser envolvidos por uma cobertura/camada que resiste às tentativas de acesso físico ao módulo. Esta cobertura/camada que resiste às violações possui o intuito de deter a observação, sondagem ou manipulação direta do módulo, e portanto, sua remoção deve resultar em danos severos ao módulo criptográfico tornando inutilizável.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.9.01: Verificar se a documentação técnica descreve os materiais que compõem a(s) cobertura(s)/camada(s) resistente(s) à violação que envolve(m) os principais componentes do módulo criptográfico.

EN.III.5.9.02: Inspecionar o módulo criptográfico por meio de equipamentos específicos e caracterizar fisicamente a cobertura/camada resistente à violação que envolve os principais componentes do módulo criptográfico.

EN.III.5.9.03: Realizar tentativas de observação, sondagem e manipulação do módulo criptográfico por meio de técnicas específicas, de forma a deixar os componentes do módulo criptográfico intactos. Após tentativas de observação, sondagem e manipulação do módulo criptográfico verificar se os principais componentes do módulo criptográfico sofreram danos e/ou se tornaram inutilizáveis.

REQUISITO III.5.10: A cobertura/camada que resiste às violações dos componentes do módulo criptográfico deve ser rígida e opaca ao espectro de luz visível.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.10.01: Verificar se a documentação técnica descreve a opacidade e rigidez da(s) cobertura(s)/camada(s) resistente(s) às violações do módulo criptográfico.

EN.III.5.10.02: Inspecionar o módulo criptográfico por meio de equipamentos específicos e caracterizar a opacidade da cobertura/camada resistente às violações físicas.

EN.III.5.10.03: Realizar tentativas de sondagem ou observação no módulo criptográfico por meio de técnicas específicas e verificar se qualquer informação pode ser obtida a respeito do módulo.

2.1.5.4 Requisitos específicos de proteção que detecta e responde à violação

REQUISITO III.5.11: A cobertura ou camada que envolve os principais componentes do módulo criptográfico deve possuir mecanismos que detectam tentativas de acesso físico ao módulo. Estes mecanismos possuem o intuito de deter a observação, sondagem ou manipulação direta do módulo, e portanto, a ativação de tais mecanismos deve resultar na destruição de informações críticas armazenadas em sua memória, como por exemplo, chaves criptográficas ou parâmetros críticos de segurança.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.5.11.01: Verificar se a documentação técnica descreve os mecanismos que detectam tentativas de acesso físico ao módulo criptográfico.

EN.III.5.11.02: Inspecionar o módulo criptográfico por meio de equipamentos específicos e caracterizar fisicamente os mecanismos que detectam tentativas de acesso físico ao módulo criptográfico.

EN.III.5.11.03: Realizar tentativas de observação, sondagem e manipulação do módulo criptográfico por meio de técnicas específicas, de forma a não ativar os sensores que detectam acesso físico ao módulo. Após tentativas de observação, sondagem e manipulação do módulo criptográfico verificar se existe a possibilidade de obter acesso físico aos componentes do módulo sem a ativação dos sensores.

2.1.6 Ambiente operacional

REQUISITO III.6.1: [FIPS 140-2, 4.6] A documentação deve especificar o ambiente operacional utilizado pelo módulo criptográfico, incluindo o sistema operacional (SO) utilizado pelo módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.6.1.01: Verificar se a documentação descreve o ambiente operacional em que o módulo opera.

REQUISITO III.6.2: [FIPS 140-2, 4.6] No caso em que o sistema operacional (SO) utilizado pelo módulo criptográfico já foi homologado em relação a alguma norma internacional ou mesmo nacional como FIPS 140-2 da NIST, *Common Criteria* da ISO/IEC ou outra, a PI deve fornecer documentação dessa homologação.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.6.2.01: Verificar se a documentação descreve sobre alguma homologação já efetuada do sistema operacional (SO) utilizado pelo módulo criptográfico por alguma norma internacional ou mesmo nacional como FIPS 140-2 da NIST, Common Criteria da ISO/IEC ou outra.

2.1.6.1 Ambiente operacional não modificável

OBSERVAÇÃO: [FIPS 140-2, 4.6] Se o ambiente operacional for um "Ambiente Operacional não modificável" não existem requisitos de segurança associados ao ambiente operacional.

2.1.6.2 Ambiente operacional modificável

Módulos criptográficos que utilizam este tipo de ambiente devem atender aos requisitos de segurança descritos a seguir.

REQUISITO III.6.3: [FIPS 140-2 nível 2, 4.6] Para proteger dados em texto claro, software e *firmware*, chaves criptográficas, PCS e dados de autenticação, o mecanismo de controle de acesso (vide seção 3.3.1) deve ser configurado para propiciar as seguintes ações:

- Especificar o conjunto de papéis que podem ativar a execução do software e *firmware* criptográficos armazenados;
- Especificar o conjunto de papéis que podem modificar (isto é, escrever, substituir ou apagar) os seguintes componentes de software ou *firmware* que estão armazenados no módulo: programas criptográficos, dados criptográficos (chaves criptográficas e dados de auditoria, por exemplo), PCS e dados em texto claro;
- Especificar o conjunto de papéis que podem ler os seguintes componentes armazenados no módulo: dados criptográficos (chaves criptográficas e dados de auditoria, por exemplo), PCS e dados em texto claro;
- Especificar o conjunto de papéis que podem inserir chaves criptográficas e PCS.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.6.3.01: Verificar se a documentação especifica como o mecanismo de controle de acesso discreto é configurado para atender as ações citadas no **REQUISITO III.6.3.**

EN.III.6.3.02: Para um papel com privilégios, executar componentes criptográficos como software ou *firmware* para verificar a configuração correta dos mecanismos de controle de acesso do sistema operacional**.**

EN.III.6.3.03: Para um papel sem privilégios, tente executar componentes criptográficos como software ou *firmware* para verificar a configuração correta dos mecanismos de controle de acesso do sistema operacional**.** Não deve ser permitido executar esses componentes.

EN.III.6.3.04: Para um papel com privilégios, modificar os seguintes componentes de software ou *firmware* do módulo criptográfico armazenados dentro da fronteira criptográfica**:**

- Programas criptográficos;
- Dados criptográficos (ex. chaves criptográficas);
- PCS;
- Dados em texto claro.

EN.III.6.3.05: Para um papel sem privilégios, tente modificar componentes criptográficos como software e *firmware*.

EN.III.6.3.06: Para um papel com privilégios, ler os seguintes componentes de software ou *firmware* do módulo criptográfico armazenados dentro da fronteira criptográfica**:**

- Dados criptográficos (ex. chaves criptográficas);
- PCS;
- Dados em texto claro.

EN.III.6.3.07: Para um papel sem privilégios, tente ler os componentes criptográficos de software ou *firmware*.

EN.III.6.3.08: Para um papel com privilégios, inserir chaves criptográficas e PCS.

EN.III.6.3.09: Para um papel sem privilégios, tente inserir chaves criptográficas e PCS.

REQUISITO III.6.4: [FIPS 140-2 nível 2, 4.6] O SO deve impedir acesso por meio de outros processos nas chaves privadas e secretas em texto claro, PCS e valores intermediários de geração de chaves enquanto o módulo estiver executando e operacional.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.6.4.01: Verificar se a documentação especifica o mecanismo usado para garantir que nenhum outro processo pode acessar chaves privadas e secretas em texto claro, PCS e valores intermediários de geração de chaves enquanto o módulo estiver executando e operacional.

EN.III.6.4.02: Executar funções criptográficas e tentar, ao mesmo tempo, acessar chaves privadas e secretas em texto claro, PCS e valores intermediários de geração de chaves.

REQUISITO III.6.5: [FIPS 140-2 nível 2, 4.6] O SO deve prover mecanismo de auditoria para registrar modificações, acessos, apagamentos e adições nos dados criptográficos e PCS.

- Eventos que devem ser registrados pelo mecanismo de auditoria:
  - Tentativas de prover entradas inválidas para funções do "Oficial de Segurança";
  - Adição de um operador para o papel de "Oficial de Segurança";
  - Remoção de um operador do papel de "Oficial de Segurança".
- O mecanismo de auditoria deve ser capaz de auditar os seguintes eventos:
  - Operações de manipulação de dados de auditoria armazenados;
  - Requisições para uso de mecanismos de gerenciamento em dados de autenticação;
  - Uso de uma função relevante ou crítica, do ponto de vista de segurança, do "Oficial de Segurança";
  - Requisições para acesso a dados de autenticação de operador;
  - Uso de um mecanismo de autenticação (*login*, por exemplo);
  - Requisições para assumir o papel de "Oficial de Segurança";
  - Associação e retirada de uma função para o papel de "Oficial de Segurança".

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.6.5.01: Verificar se a documentação especifica todos os eventos citados no **REQUISITO III.6.5** que são auditáveis pelo mecanismo de auditoria do módulo criptográfico.

EN.III.6.5.02: Ativar o mecanismo de auditoria e registrar os eventos auditáveis. Verificar o *log* de auditoria do sistema para determinar se todos os eventos foram auditados.

REQUISITO III.6.6: [FIPS 140-2 nível 2, 4.6] Todas as chaves criptográficas e PCSs, dados de autenticação, entradas de controle e saídas de status devem comunicar através de um mecanismo confiável que utilize portas físicas de I/O dedicadas ou caminho confiável.

Procedimentos de ensaio para NSH 1:

EN.III.6.8.01: Verificar se a documentação especifica um mecanismo confiável que utilize portas físicas de I/O dedicadas ou caminho confiável para todas as chaves criptográficas e PCSs, dados de autenticação, entradas de controle e saídas de status.

Procedimentos de ensaio para NSH 2 e 3:

EN.III.6.8.02: Utilizar um mecanismo confiável que utilize portas físicas de I/O dedicadas ou caminho confiável para comunicar todas as chaves criptográficas e PCSs, dados de autenticação, entradas de controle e saídas de status.

EN.III.6.8.03: Para cada entrada e saída identificada no ensaio **EN.III.6.8.01,** inserir ou gerar uma informação de saída via um mecanismo não confiável (ex. texto em claro).

RECOMENDAÇÃO III.6.1: [FIPS 140-2 nível 2, 4.6] Acrescentando os requisitos de auditoria, os seguintes eventos devem ser armazenados por mecanismos de auditoria:

- Tentativa de usar uma função de caminho confiável (*read, write, open e close*);
- identificação da origem e do destino de um caminho confiável.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.6.1.01: Verificar se a documentação inclui os eventos de auditoria na tentativa de usar uma função de caminho confiável e identificação da origem e do destino de um caminho confiável.

EN.REC.III.6.1.02: Ativar o mecanismo de auditoria e executar as ações para gerar os eventos de auditoria citados na **RECOMENDAÇÃO III.6.1**. Verificar o *log* de auditoria do sistema para determinar se esses eventos foram auditados.

2.1.7 Gerenciamento de chaves criptográficas

REQUISITO III.7.1: [FIPS 140-2, 4.7] Chaves secretas, chaves assimétricas privadas e PCSs devem estar protegidas dentro do módulo contra divulgação, modificação e substituição não autorizada.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.1.01: Analisar a documentação referente a este requisito, verificando como chaves criptográficas e PCSs são protegidos contra divulgação, modificação e substituição não autorizada.

EN.III.7.1.02: Tentar obter acesso às chaves secretas, às chaves privadas e PCS para os quais não está autorizado, usando métodos específicos (por exemplo, invocando um comando de leitura ao arquivo que contém uma chave secreta). O módulo deve negar o acesso ou permitir somente o acesso aos dados cifrados ou protegidos de outra forma.

EN.III.7.1.03: Tentar modificar ou substituir as chaves secretas, as chaves privadas e PCSs para os quais não estão autorizados, usando métodos específicos. Verificar que o módulo não permite que as chaves secretas, privadas e PCSs utilizados por serviços criptográficos sejam modificados ou substituídos.

REQUISITO III.7.2: [FIPS 140-2, 4.7] Chaves assimétricas públicas devem estar protegidas dentro do módulo contra modificação e substituição não autorizada.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.2.01: Analisar a documentação referente a este requisito, verificando como chaves assimétricas públicas são protegidas contra modificação e substituição não autorizada.

EN.III.7.2.02: Tentar modificar ou substituir as chaves assimétricas públicas para as quais não está autorizado, usando métodos específicos. Verificar que o módulo não permite que as chaves assimétricas públicas sejam modificadas ou substituídas.

REQUISITO III.7.3: [FIPS 140-2, 4.7] A documentação deve especificar todas as chaves criptográficas, seus componentes e PCSs empregados pelo módulo.

Procedimentos de ensaio para NSH 1, 2 e 3:
EN.III.7.3.01: Verificar se a documentação atende ao **REQUISITO III.7.3.**

REQUISITO III.7.4: [requisito complementar ao FIPS 140-2] A documentação deve especificar quais métodos são usados pelo módulo criptográfico para proteger chaves secretas, chaves privadas e PCSs contra divulgação, modificação e substituição não autorizada (tratado no ensaio EN.III.7.1.01).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.4.01: Verificar se a documentação atende ao **REQUISITO III.7.4.**

REQUISITO III.7.5: [requisito complementar ao FIPS 140-2] A documentação deve especificar quais métodos são usados pelo módulo criptográfico para proteger chaves públicas contra modificação e substituição não autorizada (tratado no ensaio EN.III.7.1.01).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.5.01: Verificar se a documentação atende ao **REQUISITO III.7.5.**

2.1.8 Geradores de números aleatórios

REQUISITO III.7.6: [FIPS 140-2, 4.7.1] Algoritmos RNG determinísticos aprovados pela família de padrões FIPS devem ser usados para geração de chaves utilizadas em funções criptográficas aprovadas pelo Comitê Gestor da ICP-Brasil (ver Figura 1).

Procedimentos de ensaio para NSH 1:

EN.III.7.6.01: Analisar a documentação referente a este requisito, verificando quais são os algoritmos RNG determinísticos usados 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.III.7.6.02: Por meio de uma ferramenta específica que poderia utilizar uma interface disponível 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, será avaliado se o comportamento estatístico dos algoritmos RNG determinísticos poderá ser executado nos NSHs 2 ou 3.

EN.III.7.6.03: Por meio de uma ferramenta específica que poderia utilizar uma interface disponível pela PI (por exemplo, API), realizar testes que permitam verificar o comportamento do algoritmo RNG determinístico implementado pelo módulo criptográfico, conforme listados no FIPS 140-2 Anexo C. Caso não exista algum tipo de interface que permita a realização deste ensaio, será avaliado se o comportamento, conforme listado no FIPS 140-2 dos algoritmos RNG determinísticos poderá ser executado nos NSHs 2 ou 3.
Procedimentos de ensaio para NSH 2:

EN.III.7.6.04: Verificar, por análise direta do código-fonte dos algoritmos RNG determinísticos aprovados pela família de padrões FIPS, se tais algoritmos implementados estão em conformidade com a documentação.

Procedimentos de ensaio para NSH 3:

EN.III.7.6.05: Verificar, por análise direta do código-fonte do módulo criptográfico, se o algoritmo implementado RNG determinístico aprovado pela família de padrões FIPS é utilizado para geração de chaves definidas em funções criptográficas aprovadas.

REQUISITO III.7.7: [FIPS 140-2, 4.7.1] Algoritmos RNG não aprovados pela família de padrões FIPS devem ser usados somente para gerar sementes para algoritmos de RNG determinísticos aprovados ou vetores de inicialização (IV) de funções criptográficas aprovadas pelo Comitê Gestor da ICP-Brasil (ver Figura 1).

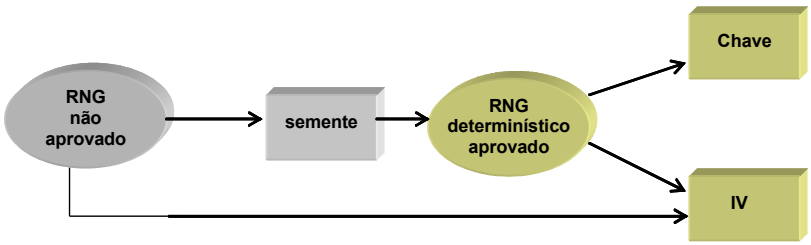

Figura 1. Geradores de números aleatórios

Procedimentos de ensaio para NSH 1:

EN.III.7.7.01: Analisar a documentação referente a este requisito, verificando quais são os algoritmos RNG não aprovados pela família de padrões FIPS usados pelo módulo criptográfico como, por exemplo, geradores tipo TRNG em hardware.

EN.III.7.7.02: Por meio de uma ferramenta específica que poderia utilizar uma interface disponível 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, será avaliado se o comportamento estatístico dos algoritmos RNG não aprovados poderá ser executado nos NSHs 2 ou 3.

Procedimentos de ensaio para NSH 2:

EN.III.7.7.03: Verificar, por análise direta do código-fonte dos algoritmos RNG não aprovados pela família de padrões FIPS, se tais algoritmos implementados estão em conformidade com a documentação.

Procedimentos de ensaio para NSH 3:

EN.III.7.7.04: Verificar, por análise direta do código-fonte do módulo criptográfico, 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 definidos em funções criptográficas aprovadas.

REQUISITO III.7.8: [FIPS 140-2, 4.7.1] A documentação deve especificar cada método de RNG empregado pelo módulo, seja ele aprovado ou não pelo padrão FIPS.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.8.01: Verificar se a documentação atende ao **REQUISITO III.7.8.**

2.1.9 Geração de chaves criptográficas

REQUISITO III.7.9: [FIPS 140-2, 4.7.2] O módulo deve usar somente os métodos aprovados pela família de padrões FIPS para a geração de chaves criptográficas. Se um dos métodos de geração de chaves criptográficas necessitar como entrada do resultado de um algoritmo RNG, então o algoritmo RNG utilizado também deve ser aprovado pela família de padrões FIPS.

Procedimentos de ensaio para NSH 1:

EN.III.7.9.01: Analisar a documentação referente a este requisito, verificando quais são os métodos de geração de chaves criptográficas usados pelo módulo, e ainda, se tais métodos são ou não aprovados pela família de padrões FIPS.

Procedimentos de ensaio para NSH 2:

EN.III.7.9.02: Verificar, por análise direta do código-fonte dos métodos de geração de chaves, se tais métodos implementados estão em conformidade com a documentação.
Procedimentos de ensaio para NSH 3:

EN.III.7.9.03: Verificar, por análise direta do código-fonte do módulo criptográfico, 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, utilizem somente algoritmos RNG aprovados pela família de padrões FIPS.

REQUISITO III.7.10: [FIPS 140-2, 4.7.2] O esforço de comprometer a segurança de um método de geração de chaves criptográficas deve ser, no mínimo, igual ao esforço de determinar o valor da chave gerada.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.10.01: Verificar se a documentação descreve o esforço necessário para comprometer a segurança de um método de geração de chaves criptográficas.

EN.III.7.10.02: Determinar o nível de clareza, raciocínio e exatidão de qualquer argumento ou parâmetro fornecido, verificando a existência de incertezas, pontos obscuros ou ambiguidades que possam comprometer o entendimento da documentação.

REQUISITO III.7.11: [FIPS 140-2, 4.7.2] Se uma semente for inserida como entrada durante o processo de geração de chaves, então a entrada desta semente deve atender aos requisitos especificados na seção 2.1.9.2(“Importação e Exportação de Chaves Criptográficas”).

Nota: Este requisito é testado como parte do **REQUISITO III.7.15.**

REQUISITO III.7.12: [FIPS 140-2, 4.7.2] A documentação deve especificar cada um dos métodos de geração de chaves criptográficas empregados pelo módulo (aprovados ou não pela família de padrões FIPS).

Nota: Este requisito é testado como parte do **REQUISITO III.7.9 (EN.III.7.9.01).**

2.1.9.1 Requisitos específicos de geração de chaves criptográficas

REQUISITO III.7.13: Quando geradas internamente ao módulo criptográfico, chaves criptográficas devem ser, obrigatoriamente, configuradas com um dos seguintes atributos: exportável ou não exportável.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.13.01: Verificar se a documentação descreve que chaves criptográficas geradas internamente ao módulo criptográfico, devem ser, obrigatoriamente, configuradas como exportável ou não exportável.

EN.III.7.13.02: Gerar chaves criptográficas internamente ao módulo criptográfico e verificar se as mesmas estão configuradas com os atributos de exportável ou não exportável.

2.1.9.2 Importação e exportação de chaves criptográficas

REQUISITO III.7.14: [FIPS 140-2 níveis 1 e 2, 4.7.4] Uma chave criptográfica simétrica ou assimétrica privada quando importada ou exportada do módulo criptográfico utilizando um método automático deve ser cifrada utilizando algoritmo aprovado pela família de padrões FIPS.

Procedimentos de ensaio para NSH 1:

EN.III.7.14.01: Verificar se a documentação descreve como os processos de importação e exportação são realizados para chaves criptográficas privadas simétricas ou assimétricas.

EN.III.7.14.02: Verificar, por meio de ferramenta específica, se o processo de importação de chave assimétrica possui proteção da chave assimétrica privada conforme a documentação fornecida. Por exemplo, por meio de PKCS#12.

EN.III.7.14.03: Quando aplicável, verificar, por meio de ferramenta específica, se os processos de importação e exportação de chave simétrica apresentam indícios de proteção das chaves conforme a documentação fornecida. Caso não seja possível a realização deste ensaio, será avaliada se a verificação de proteção da chave simétrica nos processos de importação e exportação poderá ser executada nos NSHs 2 ou 3.

Procedimentos de ensaio para NSH 2:

EN.III.7.14.04: Verificar, por análise direta do código-fonte do componente de importação/exportação de chaves, se tal componente protege as chaves nos processos de importação e exportação pelo módulo criptográfico.

Procedimentos de ensaio para NSH 3:

EN.III.7.14.05: Verificar, por análise direta do código-fonte do módulo criptográfico, se somente algoritmos aprovados pela família de padrões FIPS são usados na proteção de chaves durante os processos de importação e exportação pelo módulo criptográfico.

REQUISITO III.7.15: [FIPS 140-2, 4.7.4] Se o processo de geração de chaves necessitar da importação ou exportação de uma semente, esta semente deve ser importada ou exportada usando os mesmos critérios aplicados às chaves criptográficas.

Procedimentos de ensaio para NSH 1:

EN.III.7.15.01: Verificar se a documentação descreve como os processos de importação e exportação são realizados para sementes.

EN.III.7.15.02: Verificar, por meio de ferramenta específica, se os processos de importação e exportação de sementes possui proteção conforme a documentação fornecida. Por exemplo, cifrado com par de chaves.

Procedimentos de ensaio para NSH 2:

EN.III.7.15.03: Verificar, por análise direta do código-fonte do componente de importação/exportação de sementes, se tal componente protege as sementes nos processos de importação e exportação pelo módulo criptográfico.

Procedimentos de ensaio para NSH 3:

EN.III.7.15.04: Verificar, por análise direta do código-fonte do módulo criptográfico, se somente algoritmos aprovados pela família de padrões FIPS são usados na proteção de sementes durante os processos de importação e exportação pelo módulo criptográfico.

REQUISITO III.7.16: [FIPS 140-2, 4.7.4] O módulo criptográfico deve associar a chave importada ou exportada à entidade correta a qual a chave está vinculada.
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.16.01: Analisar se a documentação descreve como o módulo criptográfico associa a chave importada ou exportada à sua entidade correta.

EN.III.7.16.02: Caso sejam aplicáveis as operações de exportação e importação de chaves para cada chave presente no módulo criptográfico, primeiro exportar uma chave enquanto assume uma dada entidade por meio de ferramenta específica. Em seguida, assumir uma entidade diferente da primeira e tentar importar a chave exportada no módulo, verificando que a inserção não deve ser possível.

EN.III.7.16.03: Caso sejam aplicáveis as operações de exportação e importação de chaves, para cada chave presente no módulo criptográfico, primeiro importar uma chave enquanto assume uma dada entidade por meio de ferramenta específica. Em seguida, assumir uma entidade diferente da primeira e tentar exportar a chave importada no módulo, verificando que a exportação não deve ser possível.

REQUISITO III.7.17: [FIPS 140-2, 4.7.4] A documentação deve especificar os métodos de importação e exportação de chaves criptográficas empregados pelo módulo (métodos aprovados ou não pela família de padrões FIPS).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.17.01: Verificar se a documentação atende ao **REQUISITO III.7.17.**

REQUISITO III.7.18: [FIPS 140-2, 4.7.4] Chaves importadas manualmente devem ser verificadas durante a entrada no módulo criptográfico utilizando o teste especificado na seção 2.1.11.2

Nota: Este requisito é testado como parte do **REQUISITO III.9.13.**

REQUISITO III.7.19: [FIPS 140-2, 4.7.4, níveis de segurança 2 e 3] Chaves secretas e privadas importadas utilizando métodos manuais devem entrar no módulo criptográfico ou sair do módulo criptográfico

1. Cifradas;
2. Utilizando procedimentos de compartilhamento de conhecimento (*split knowledge*).

Procedimentos de ensaio para NSH 2 e 3:

EN.III.7.19.01: Verificar se a documentação atende ao **REQUISITO III.7.19.**

EN.III.7.19.02: Se métodos manuais são usados para estabelecer chaves secretas e privadas importadas, então verificar que essas chaves entrem do módulo criptográfico cifradas ou utilizando procedimentos de compartilhamento de conhecimento (*split knowledge*).

EN.III.7.19.03: Se métodos manuais são usados para estabelecer chaves secretas e privadas importadas, então verificar que essas chaves saiam do módulo criptográfico cifradas ou utilizando procedimentos de compartilhamento de conhecimento (*split knowledge*).

REQUISITO III.7.20: [FIPS 140-2, 4.7.4, níveis de segurança 2 e 3] Caso o compartilhamento de conhecimento (*split knowledge*) estiver sendo utilizado para entrada de chaves secretas e privadas:

- O módulo criptográfico deve autenticar cada operador inserindo ou extraindo cada componente de chaves separadamente.
- Componentes de chaves criptográficas em texto claro devem ser inseridos ou extraídos diretamente no módulo criptográfico por meio de um caminho confiável.

- No mínimo dois componentes de chaves devem ser necessários para recompor a chave criptográfica original.
- A documentação deve descrever tecnicamente que, se o conhecimento de *n* componentes de chaves for necessário para recompor a chave, o conhecimento de *n-1* componentes não fornece nenhuma informação sobre a chave original além do tamanho da chave.

Procedimentos de ensaio para NSH 2 e 3:

EN.III.7.20.01: Verificar se a documentação atende ao **REQUISITO III.7.20.**

EN.III.7.20.02: Verificar se a autenticação é feita para cada componente de chave e se a autenticação está de acordo com os procedimentos documentados de entrada e saída de chaves.

EN.III.7.20.03: Inserir cada componente de chave usando procedimentos de *split knowledge* e verificar se cada operador, inserindo um componente da chave, está autenticado.

EN.III.7.20.04: Extrair cada componente de chave usando procedimentos de *split knowledge* e verificar se cada operador, extraindo um componente da chave, está autenticado.

EN.III.7.20.05: Inserir cada componente de chave criptográfica em texto claro diretamente no módulo criptográfico usando procedimentos de *split knowledge* e verificar se foi utilizado um caminho confiável para tal procedimento.

EN.III.7.20.06: Extrair cada componente de chave criptográfica em texto claro diretamente do módulo criptográfico usando procedimentos de *split knowledge* e verificar que foi utilizado um caminho confiável para tal procedimento.

EN.III.7.20.07: Verificar na documentação o número de componentes da chave que são necessários para recompor a chave original.

EN.III.7.20.08: Verificar se os componentes da chave disponíveis são suficientes para recompor a chave criptográfica original.

EN.III.7.20.09: Verificar a veracidade técnica da documentação sobre o fato do conhecimento de *n* componentes de chaves ser necessário para recompor a chave e o conhecimento de *n-1* componentes não fornecer nenhuma informação sobre a chave original além do tamanho da chave.

2.1.9.3 Requisitos específicos de exportação de chaves criptográficas

REQUISITO III.7.21: Deve ser possível configurar no módulo criptográfico com atributo não exportável uma chave criptográfica assimétrica privada, para fins de assinatura digital, compatível com certificados digitais ICP-Brasil de tipo A3 ou A4. Uma vez definido tal atributo como não exportável, não deve ser possível alterar seu valor para exportável.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.21.01: Verificar se a documentação atende ao **REQUISITO III.7.21.**

EN.III.7.21.02: Configurar no módulo criptográfico, com atributo não exportável, uma chave criptográfica assimétrica privada, para fins de assinatura digital, compatível com certificados digitais ICP-Brasil de tipo A3 ou A4.

EN.III.7.21.03: Uma vez definido tal atributo como não exportável, tentar alterar seu valor para exportável. Se isso for possível, o requisito não foi atendido.

REQUISITO III.7.22.1: Se o módulo criptográfico suporta chave criptográfica simétrica, então deve ser possível configurar no módulo criptográfico com atributo não exportável uma chave criptográfica simétrica. Uma vez definido tal atributo como não exportável, não deve ser possível alterar seu valor para exportável.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.22.1.01: Verificar se a documentação atende ao **REQUISITO III.7.22.1.**

EN.III.7.22.1.02: Configurar no módulo criptográfico, com atributo não exportável, uma chave criptográfica simétrica.

EN.III.7.22.1.03: Uma vez definido tal atributo como não exportável, tentar alterar seu valor para exportável. Se isso for possível, o requisito não foi atendido.

REQUISITO III.7.22.2: Deve ser possível configurar no módulo criptográfico com atributo não exportável uma chave criptográfica assimétrica privada, para fins de sigilo, compatível com certificados digitais ICP-Brasil de tipo S3 ou S4. Uma vez definido tal atributo como não exportável, não deve ser possível alterar seu valor para exportável.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.22.2.01: Verificar se a documentação atende ao **REQUISITO III.7.22.2.**

EN.III.7.22.2.02: Configurar no módulo criptográfico, com atributo não exportável, uma chave criptográfica assimétrica privada, compatível com certificados digitais ICP-Brasil de tipo S3 ou S4.

EN.III.7.22.2.03: Uma vez definido tal atributo como não exportável, tentar alterar seu valor para exportável. Se isso for possível, o requisito não foi atendido.

REQUISITO III.7.23: Chaves assimétricas públicas devem ser exportáveis do módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.23.01: Verificar se a documentação atende ao **REQUISITO III.7.23.**

EN.III.7.23.02: Exportar chaves assimétricas públicas do módulo criptográfico e verificar a integridade da operação.

2.1.9.4 Atribuição de chaves

REQUISITO III.7.24: [FIPS 140-2, 4.7.3] Quando aplicável, a documentação deve especificar os métodos de atribuição de chaves (conforme definido no item 3.7.4) empregados pelo módulo criptográfico (automático, manual ou combinação dos anteriores).
Procedimentos de ensaio para NSH 1, 2 e 3:
EN.III.7.24.01: Verificar se a documentação atende ao **REQUISITO III.7.24.**

REQUISITO III.7.25: [FIPS 140-2, 4.7.3] Se métodos de atribuição de chaves (conforme definido no item 3.7.4) são empregados pelo módulo criptográfico, então somente os métodos de atribuição de chaves aprovados pela família de padrões FIPS devem ser usados.

Procedimentos de ensaio para NSH 1:

EN.III.7.25.01: Analisar a documentação referente a este requisito, verificando quais são os algoritmos de atribuição de chaves presentes no módulo criptográfico, e ainda, se tais algoritmos constam no Anexo D do FIPS PUB 140-2.
Procedimentos de ensaio para NSH 2:

EN.III.7.25.02: Verificar, por análise direta do código-fonte dos métodos de atribuição de chaves, se tais métodos implementados no módulo criptográfico estão em conformidade com a documentação.

Procedimentos de ensaio para NSH 3:

EN.III.7.25.03: Verificar, por análise direta do código-fonte do módulo criptográfico, se somente métodos de atribuição de chaves aprovados pela família de padrões FIPS são usados.

2.1.9.5 Armazenamento de chaves criptográficas

REQUISITO III.7.26: [FIPS 140-2, 4.7.5] Chaves criptográficas devem ser armazenadas dentro do módulo criptográfico em texto claro ou de forma cifrada.

Procedimentos de ensaio para NSH 1:

EN.III.7.26.01: Analisar a documentação referente a este requisito, verificando, para cada chave armazenada:

- O modo de armazenamento da chave dentro do módulo (texto claro e cifrado);
- O tipo e o identificador da chave armazenada dentro do módulo;
- A localização do armazenamento da chave dentro do módulo;
- O algoritmo criptográfico utilizado para cifrar a chave dentro do módulo.

Procedimentos de ensaio para NSH 2 e 3:

EN.III.7.26.02: Verificar, por análise direta do código-fonte do componente de armazenamento de chaves, se as chaves criptográficas são armazenadas em texto claro ou de forma cifrada.

REQUISITO III.7.27: [FIPS 140-2, 4.7.5] Chaves privadas e secretas em texto claro não devem ser acessíveis por operadores não autorizados.
Nota: Este requisito é testado como parte do **REQUISITO III.7.1.**

REQUISITO III.7.28: [FIPS 140-2, 4.7.5] O módulo criptográfico deve associar a cada chave (simétrica ou assimétrica) armazenada o seu respectivo operador (pessoa, grupo, processo, servidor, etc).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.7.28.01: Verificar se a documentação descreve como o módulo criptográfico associa cada chave armazenada o seu respectivo operador.

EN.III.7.28.02: Para cada chave K_i armazenada no módulo criptográfico, é preciso assumir o operador desta chave por meio de ferramenta específica. Em seguida, é preciso assumir um operador diferente do primeiro e tentar executar funções criptográficas com a chave K_i, verificando que esta execução não deve ser possível.

REQUISITO III.7.29: [FIPS 140-2, 4.7.5] A documentação deve especificar os métodos de armazenamento de chaves criptográficas empregados pelo módulo.

Nota: Este requisito é testado como parte do **REQUISITO III.7.26 (EN.III.7.26.01).**

2.1.9.6 Sobrescrita do valor de chaves criptográficas com zeros binários

REQUISITO III.7.30: [FIPS 140-2, 4.7.6] O módulo deve prover métodos para sobrescrever com zeros binários os valores das chaves simétricas, chaves assimétricas privadas e PCSs.

Procedimentos de ensaio para NSH 1:

EN.III.7.30.01: Analisar a documentação referente a este requisito, verificando se os seguintes itens estão especificados:

- Técnicas de sobrescrita;
- Restrições de sobrescrita;
- Chaves criptográficas e PCSs que são sobrescritos;
- Análise da robustez das técnicas de sobrescrita perante o comprometimento de chaves e PCSs;
- Todas as chaves simétricas, chaves assimétricas privadas e PCSs são sobrescritos.

Procedimentos de ensaio para NSH 2:

EN.III.7.30.02: Executar a operação de sobrescrita em chaves armazenadas no módulo criptográfico. Após completar a operação de sobrescrita, verificar se não é possível obter acesso às chaves eliminadas.

EN.III.7.30.03: Executar a operação de sobrescrita em uma chave armazenada no módulo criptográfico. Após a conclusão desta operação de sobrescrita, verificar se a destruição foi realizada em um tempo que não é suficiente para comprometer a chave criptográfica eliminada.

EN.III.7.30.04: Verificar, por análise direta do código-fonte do componente de sobrescrita de chaves, se o método de sobrescrita é adequado perante o comprometimento de chaves e PCSs.

Procedimentos de ensaio para NSH 3:

EN.III.7.30.05: Verificar, por análise direta do código-fonte do módulo criptográfico, se a ação de sobrescrita com zeros binários ocorre quando chaves simétricas, chaves assimétricas privadas e PCSs são eliminados.

REQUISITO III.7.31: [FIPS 140-2, 4.7.5] A documentação deve especificar os métodos de sobrescrita de chaves criptográficas com zeros binários que são empregados pelo módulo.

Nota: Este requisito é testado como parte do **REQUISITO III.7.30 (EN.III.7.30.01).**

2.1.10 Interferência/compatibilidade eletromagnética

RECOMENDAÇÃO III.8.1: [requisito FIPS 140-2, item 4.8] É recomendado à parte interessada apresentar documentação comprovando conformidade do equipamento às normas de EMI/EMC para equipamentos de tecnologia da informação compatíveis com as normas reconhecidas internacionalmente (i.e, IEC CISPR 22 E 24, FCC CFR 47).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.8.1.01: Analisar e verificar se a documentação apresenta certificado ou relatório de ensaio que ateste a conformidade do equipamento às normas de EMI/EMC para equipamentos de tecnologia da informação compatíveis com as normas reconhecidas internacionalmente.

RECOMENDAÇÃO III.8.2: [requisito FIPS 140-2, item 4.8] É recomendado à parte interessada apresentar documentação constando o nome da organização/laboratório responsável onde foi obtida a certificação de conformidade EMI/EMC para o equipamentos de tecnologia da informação. Além disso, a documentação deve citar o órgão regulador que o laboratório está credenciado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.8.2.01: Analisar e verificar se a documentação apresenta nome do laboratório responsável onde foi obtida, para o equipamento em processo de homologação, a certificação de conformidade EMI/EMC para equipamentos de tecnologia da informação, além de citar o órgão regulador ao qual este laboratório está credenciado.

2.1.11 Auto-testes

REQUISITO III.9.1: [FIPS 140-2, 4.9] A documentação do módulo criptográfico deve especificar os seguintes itens:

- Os auto-testes realizados pelo módulo;
- O estado de erro que o módulo criptográfico pode entrar quando um auto-teste falha; e
- As condições e ações necessárias para sair dos estados de erro e reiniciar a operação normal do módulo criptográfico (por exemplo, isto poderia incluir a manutenção ou retorno do módulo ao fabricante para fins de reparo).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.9.1.01: Verificar se a documentação atende ao **REQUISITO III.9.1.**

REQUISITO III.9.2: [FIPS 140-2, 4.9] Para verificar o funcionamento apropriado do módulo criptográfico, duas categorias de auto-testes devem ser realizadas:

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

O módulo poderia realizar outras categorias de auto-testes em adição àqueles especificados nas seções 2.1.11.1 e 2.1.11.2.

Procedimentos de ensaio para NSH 1:

EN.III.9.2.01: Analisar a documentação que descreve os auto-testes do módulo criptográfico, verificando os respectivos estados de erro, os eventos que podem produzir tais estados, as ações necessárias para retirar os estados de erro, e ainda, se os seguintes testes estão incluídos:

- Testes de energização
    - Teste de algoritmo criptográfico;
    - teste de integridade de software/*firmware*;
    - teste de funções críticas;
    - outros auto-testes que são executados na energização e sob demanda.
- Testes condicionais
    - Teste de consistência de par de chaves (*pairwise*), caso o módulo criptográfico gere chaves públicas e privadas;
    - Teste de carregamento do software/*firmware*;
    - Teste de entrada manual de chave;
    - Teste de gerador de números aleatórios contínuo;
    - Teste de contorno (*bypass*);
    - Outros testes condicionais.

EN.III.9.2.02: Energizar o módulo criptográfico e analisar os auto-testes realizados, verificar se não há a necessidade de qualquer intervenção por parte de um operador.

EN.III.9.2.03: Energizar o módulo criptográfico e observar o indicador emitido na interface de saída de estado. Após a observação do indicador de estado, verificar se está ou não em conformidade com a documentação fornecida.

EN.III.9.2.04: Com base nos procedimentos fornecidos pela PI, iniciar os auto-testes de energia sob demanda e verificar se está em conformidade com a documentação fornecida.

EN.III.9.2.05: Verificar se os seguintes auto-testes de energização: teste de algoritmo criptográfico, teste de integridade de software/*firmware* e teste de funções críticas são executados.

EN.III.9.2.06: Verificar se os seguintes auto-testes condicionais: teste de consistência de paridade (*pairwise*), teste de carregamento do software/*firmware*, teste de entrada manual de chave, teste de gerador de números aleatórios contínuo e teste de contorno são executados.

EN.III.9.2.07: Provocar os estados de erro dos auto-testes suportados pelo módulo criptográfico. Para cada estado de erro alcançado, executar as ações necessárias para retirar o módulo criptográfico do estado de erro alcançado e depois verificar se está ou não em conformidade com a documentação fornecida.
Procedimentos de ensaio para NSH 2 e 3:

EN.III.9.2.08: Avaliar o código-fonte do módulo criptográfico e a documentação do projeto para determinar a implementação de todos os auto-testes de energização e condicionais e se as ações necessárias para retirar o módulo criptográfico do estado de erro alcançado estão em conformidade com a documentação fornecida.

REQUISITO III.9.3: [FIPS 140-2, 4.9] Se o módulo apresentar falhas durante um auto-teste, o módulo deve ser conduzido a um estado de erro e emitir um indicador de erro via "Interface de Saída de Estado".

Procedimentos de ensaio para NSH 1:

EN.III.9.3.01: Verificar a documentação que descreve os estados de erro dos auto-testes suportados pelo módulo criptográfico, bem como o indicador de erro associado com cada estado de erro.

EN.III.9.3.02: Comparar a lista de estados de erro com aquela definida no modelo de estado finito do módulo criptográfico e verificar se há compatibilidade.

EN.III.9.3.03: Provocar os estados de erro dos auto-testes por meio de equipamento específico e analisar os indicadores de erro emitidos via "Interface de Saída de Estado". Após a obtenção dos indicadores de erro dos auto-testes, verificar se os estados e indicadores de erro estão consistentes com a documentação e o modelo de estado finito.

Procedimentos de ensaio para NSH 2 e 3:

EN.III.9.3.04: Para cada estado de erro dos auto-testes que não puder ser alcançado, avaliar o código-fonte do módulo criptográfico e a documentação do projeto para determinar o respectivo indicador de erro que seria emitido via "Interface de Saída de Estado".

REQUISITO III.9.4: [FIPS 140-2, 4.9] O módulo não deve realizar qualquer operação criptográfica enquanto o estado de erro provocado por falhas em um auto-teste persistir.

Procedimentos de ensaio para NSH 1:

EN.III.9.4.01: Analisar a documentação, sendo que as seguintes funções criptográficas devem estar incluídas na lista de funções inibidas quando o módulo criptográfico estiver num estado de erro:

- Cifragem;
- Decifração;
- Geração segura de resumos criptográficos (*secure message hashing*);
- Verificação e criação de assinaturas digitais;
- Outras operações que necessitam do uso de criptografia.

EN.III.9.4.02: Provocar os estados de erro dos auto-testes suportados pelo módulo criptográfico e, para cada estado de erro alcançado em um auto-teste, efetuar tentativas de realização de operações criptográficas específicas. Para cada tentativa realizada, verificar se as operações criptográficas não devem ser concluídas de forma bem sucedida.

EN.III.9.4.03: Verificar se quando o módulo criptográfico é conduzido a um estado de erro, não há qualquer saída de dados pela "Interface de Saída de Dados".

Procedimentos de ensaio para NSH 2 e 3:

EN.III.9.4.04: Para cada estado de erro dos auto-testes que não puder ser alcançado, avaliar o código-fonte do módulo criptográfico e a documentação do projeto para determinar se há algum tipo de controle que impeça qualquer operação criptográfica de ser realizada enquanto o estado de erro persistir.

REQUISITO III.9.5: [FIPS 140-2, 4.9] Quando um estado de erro ocorrer devido às falhas em um auto-teste, toda saída ou envio de dados via "Interface de Saída de Dados" deve ser impedido.

Procedimentos de ensaio para NSH 1:

EN.III.9.5.01: Analisar a documentação, verificar se o módulo criptográfico impede a saída ou envio de dados via "Interface de Saída de Dados" enquanto houver um estado de erro devido às falhas num auto-teste.

EN.III.9.5.02: Provocar uma falha em cada auto-teste suportado pelo módulo criptográfico e para cada estado de erro alcançado em um auto-teste, efetuar medidas de sinal por meio de um equipamento específico na "Interface de Saída de Dados". Durante a observação das medidas, verificar se há qualquer sinal sendo trafegado pela "Interface de Saída de Dados".

Procedimentos de ensaio para NSH 2 e 3:

EN.III.9.5.03: Para cada estado de erro dos auto-testes que não puder ser alcançado, avaliar o código-fonte do módulo criptográfico e a documentação do projeto, com o intuito de determinar se há algum tipo de controle que impeça que qualquer sinal trafegue pela "Interface de Saída de Dados".

2.1.11.1 Testes de energização

REQUISITO III.9.6: [FIPS 140-2, 4.9.1] Os testes de energização serão executados pelo módulo criptográfico quando o módulo é energizado (depois de ser desligado, reinicializado, reinicialização do SO, etc)

Nota: Este requisito é testado como parte do **REQUISITO III.9.7.**

REQUISITO III.9.7: [FIPS 140-2, 4.9.1] Os testes de energização serão executados automaticamente quando ocorrer a energização do módulo e sem intervenção de qualquer operador.

O módulo criptográfico deve realizar testes dos algoritmos criptográficos do tipo "resposta conhecida" para todas as funções criptográficas (cifrar, decifrar, autenticação e geração de números pseudo-aleatórios).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.9.7.01: Verificar se a documentação atende ao **REQUISITO III.9.7.**

EN.III.9.7.02: Energizar o módulo e verificar se o módulo executa os testes de energização sem qualquer intervenção de qualquer operador.

EN.III.9.7.03: Verificar se a documentação é consistente com a implementação do módulo criptográfico para os testes dos algoritmos criptográficos do tipo "resposta conhecida" para todas as funções criptográficas.

REQUISITO III.9.8: [FIPS 140-2, 4.9.1] A documentação deve listar todos os testes de funções criptográficas do tipo "resposta conhecida".

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.9.8.01: Verificar se a documentação lista todos os testes de funções criptográficas do tipo "resposta conhecida".

2.1.11.2 Testes condicionais

REQUISITO III.9.9: [FIPS 140-2, 4.9.2] Se as chaves (públicas e privadas) são utilizadas para realizar um método de transporte de chaves aprovado pelo FIPS 140-2, a chave pública deve cifrar um valor em texto claro. O valor do texto cifrado será comparado com o texto claro original. Se os dois valores são iguais o teste deve falhar. Se os dois valores forem diferentes, a

chave privada será utilizada para decifrar o texto cifrado e o valor resultante será comparado com o valor de texto claro original. Se os dois valores forem diferentes, o teste deve falhar.
Se os componentes de software e *firmware* puderem ser carregados externamente para dentro do módulo criptográfico, o seguinte teste de carregamento de software/*firmware* será executado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.9.9.01: Verificar se a documentação atende ao **REQUISITO III.9.9.**

EN.III.9.9.02: Se chaves (públicas e privadas) são utilizadas para realizar um método de transporte de chaves aprovado, o módulo criptográfico deve testar a consistência do par de chaves cifrando a chave pública em um valor em texto claro. O valor do texto cifrado será comparado ao texto claro original para verificar:

- Se os dois valores são iguais, então o módulo criptográfico deve entrar em estado de erro e mostrar um indicador de erro via interface de status.
- Se os dois valores são diferentes, então a chave privada deve ser utilizada para decifrar o texto cifrado e o resultado comparado ao texto em claro original. Se os dois valores forem diferentes, então o teste falhou.

REQUISITO III.9.10: [FIPS 140-2, 4.9.2] Um método de autenticação aprovado será utilizado para todos componentes de software e *firmware* validados quando os componentes forem carregados externamente para dentro do módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.9.10.01: Verificar se a documentação descreve um método de autenticação aprovado usado para proteger a integridade de todos os componentes de software/*firmware* carregados externamente para dentro do módulo criptográfico.

EN.III.9.10.02: Verificar se a documentação dos testes de carregamento do software e *firmware* inclui:

- Um método de autenticação aprovado usado para proteger a integridade de todos os componentes de software e *firmware* carregados externamente para dentro do módulo criptográfico**;**
- Identificação do software e *firmware* que é protegido usando o método de autenticação aprovado;
- Cálculo do método de autenticação aprovado quando o teste de carregamento é inicializado;
- Falha do auto-teste sob falha da verificação do método de autenticação aprovado.

EN.III.9.10.03: Testar o módulo modificando o software ou *firmware* a ser carregado ou o mecanismo de autenticação implementado. Iniciar os auto-testes e observar a saída pelo status da interface de saída. Se nenhum indicador mostrar que o teste de carregamento de software ou *firmware* falhou, então o ensaio falhou.

REQUISITO III.9.11: [FIPS 140-2, 4.9.2] Quando componentes de software/*firmware* são carregados externamente para dentro do módulo criptográfico, um teste de integridade será realizado. Se o resultado calculado é diferente do valor previamente calculado, o teste deve falhar e não carregar o software/firmware.

Nota: Este requisito é testado como parte do **REQUISITO III.9.10.**

Se chaves criptográficas ou componentes de chaves são colocados para dentro do módulo manualmente, os seguintes testes de entrada manual de chaves criptográficas devem ser realizados.

REQUISITO III.9.12: [FIPS 140-2, 4.9.2] Caso um código de detecção de erro for utilizado ele deve ter no mínimo 16 bits de tamanho.

Nota: Este requisito é testado como parte do **REQUISITO III.9.13.**

REQUISITO III.9.13: [FIPS 140-2, 4.9.2] Se o código de detecção de erro for utilizado, o teste deve falhar se o código de detecção de erro não puder ser verificado ou as entradas duplicadas não forem idênticas.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.9.13.01: Verificar se a documentação especifica o teste de entrada manual de chaves criptográficas.

EN.III.9.13.02: Verificar na documentação qual método é usado no teste de entrada manual de chaves criptográficas. Baseado no método usado, verificar na documentação, código e/ou *design* que especifica a implementação do teste de entrada manual de chaves criptográficas, se as seguintes informações foram incluídas:

- Códigos de detecção de erros:
  - Formato das chaves para todas as chaves de entradas manuais, incluindo os campos dos códigos de detecção de erros;
  - Descrição do algoritmo calculado do código de detecção de erro;
  - Descrição do processo de verificação;
  - Saídas esperadas no caso de sucesso ou falha nos testes.
- Entradas de chaves duplicadas:
  - As entradas de chaves duplicadas para todas as chaves de entradas manuais;
  - Descrição do processo de verificação;
  - Saídas esperadas no caso de sucesso ou falha nos testes.

EN.III.9.13.03: Para os testes de entradas de chaves manuais usando códigos de detecção de erros, realizar os seguintes testes:

- Para toda chave de entrada manual, verificar se o procedimento usado para entrar cada chave está de acordo com os procedimentos documentados, incluindo a forma como as chaves são inseridas;
- Entrar cada tipo de chave de entrada manual sem qualquer erro e observar o status da interface de saída. Se nenhum indicador for detectado ou se o indicador não corresponder ao indicador documentado para o sucesso do teste de entrada manual de chaves, então o teste falhou;
- Executar operações criptográficas com cada chave inserida para verificar se elas foram inseridas corretamente;

- Modificar o código de detecção de erros associado a cada chave de entrada manual ou modificar a própria chave e inserí-las no módulo. Observar o indicador que é obtido do status da interface de saída. Se nenhum indicador for obtido ou se o indicador não corresponder ao indicador documentado para a falha do teste de entrada manual de chaves, então o teste falhou;
- Executar operações criptográficas a cada chave que não tiver sido inserida corretamente. Cada operação, usando cada uma dessas chaves deve falhar, verificando que a chave não foi inserida.

EN.III.9.13.04: Para os testes de entradas de chaves manuais usando entradas de chaves duplicadas, realizar os seguintes testes:

- Entrar cada tipo de chave de entrada manual sem qualquer erro e observar o status da interface de saída. Se nenhum indicador for detectado ou se o indicador não corresponder ao indicador documentado para o sucesso do teste de entrada manual de chaves, então o teste falhou;
- Executar operações criptográficas com cada chave inserida para verificar que elas foram inseridas corretamente;
- Modificar a exatidão de uma das chaves de entrada manual, a primeira ou a segunda entrada duplicada, e inserí-las no módulo. Observar o indicador que é obtido do status da interface de saída. Se nenhum indicador for obtido ou se o indicador não corresponder ao indicador documentado para a falha do teste de entrada manual de chaves, então o teste falhou;
- Executar operações criptográficas a cada chave que não tiver sido inserida corretamente. Cada operação, usando cada uma dessas chaves deve falhar, verificando que a chave não foi inserida.

REQUISITO III.9.14: [FIPS 140-2, 4.9.2] Se o módulo criptográfico utiliza um método de geração de números aleatórios aprovado ou não aprovado num modo de operação aprovado, o módulo criptográfico deve realizar o teste estatístico FIPS "contínuo" do gerador de números aleatórios.

Nota: Este requisito é testado como parte do **REQUISITO III.9.15 e REQUISITO III.9.16.**

REQUISITO III.9.15: [FIPS 140-2, 4.9.2] Se cada chamada de um gerador de números aleatórios produzir blocos de n bits (onde n > 15), o primeiro bloco de n bits gerado depois da energização, inicialização ou *reset* não será utilizado, mas armazenado para comparação com o próximo bloco de n bits gerado. Cada bloco de n bits gerado em sequência deve ser comparado com o bloco previamente gerado. O teste deve falhar se qualquer dos dois blocos de n bits forem iguais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.9.15.01: Se o módulo implementa um gerador de números aleatórios, verificar se a documentação especifica o teste contínuo de gerador de números aleatórios.

EN.III.9.15.02: Se o gerador de números aleatórios produz blocos de n bits, onde n > 15, então verificar que a implementação do teste inclui:

- Armazenamento do primeiro bloco para comparação com o próximo bloco.
- Comparação de cada bloco subsequente gerado com o bloco gerado anteriormente.
- Falha do teste se dois blocos comparados forem iguais.

REQUISITO III.9.16: [FIPS 140-2, 4.9.2] Se cada chamada de um gerador de números aleatórios produzir menos que 16 bits, os primeiros n bits gerados depois da energização, inicialização ou *reset* (para algum n > 15) não serão utilizados, mas armazenados para comparação com os próximos n bits gerados. Cada subsequência de n bits gerada deve ser comparada com os n bits previamente gerados. O teste deve falhar se quaisquer das sequências comparadas de n bits forem iguais.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.9.16.01: Se o módulo implementa um gerador de números aleatórios, verificar se a documentação especifica o teste contínuo de gerador de números aleatórios.

EN.III.9.16.02: Se o gerador de números aleatórios produzir blocos menores do que 16 bits, então verificar se a implementação do teste inclui o seguinte:

- Armazenamento dos primeiros n bits, onde n > 15, para comparação com os próximos n bits gerados.
- Comparação de cada n bits subsequente gerado com os n bits gerados anteriormente.
- Falha do teste se duas sequências de n-bits comparadas forem iguais.

2.1.12 Garantia de projeto

REQUISITO III.10.1: [FIPS 140-2, 4.10] A documentação do fabricante deve descrever o sistema de gerenciamento de configuração para o módulo criptográfico, componentes do módulo criptográfico.
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.10.1.01: Verificar se a documentação descreve o sistema de gerenciamento de configuração para o módulo criptográfico e componentes do módulo criptográfico.

REQUISITO III.10.2: [FIPS 140-2, 4.10] A documentação deve listar procedimentos específicos de instalação segura e inicialização do módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.10.2.01: Verificar se a documentação lista os procedimentos específicos de instalação segura e inicialização do módulo criptográfico.

EN.III.10.2.02: Executar os procedimentos de instalação segura e inicialização do módulo criptográfico e verificar a sua acertividade.

REQUISITO III.10.3: [FIPS 140-2, 4.10] A documentação deve especificar a relação entre o projeto dos componentes de hardware, software e *firmware* do módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.10.3.01: Verificar se a documentação especifica a relação entre o projeto dos componentes de hardware, software e *firmware* do módulo criptográfico.

Nível de Segurança da Homologação 1

REQUISITO III.10.4: [FIPS 140-2, 4.10] O documento "Guia do Administrador" deve especificar:

- Funções administrativas, eventos de segurança, parâmetros de segurança, portas físicas e as interfaces lógicas do módulo criptográfico;
- Procedimentos de como administrar o módulo criptográfico de modo seguro;
- Suposições relacionadas ao comportamento do usuário que são relevantes à operação segura do módulo criptográfico.

EN.III.10.4.01: Verificar se a documentação especifica os itens do **REQUISITO III.10.4**.

REQUISITO III.10.5: [FIPS 140-2, 4.10] O documento "Guia do Usuário" deve especificar:

- As funções, portas físicas e interfaces lógicas de segurança aprovadas disponíveis para o usuário do módulo criptográfico;
- todas as responsabilidades do usuário necessárias para a operação segura do módulo criptográfico.

EN.III.10.5.01: Verificar se a documentação especifica os itens do **REQUISITO III.10.5**.

Nível de Segurança da Homologação 2

REQUISITO III.10.6: [FIPS 140-2, 4.10] Se o módulo criptográfico contém componentes de software ou *firmware*, a documentação deve especificar o código-fonte com comentários que esclareçam a correspondência dos componentes do módulo criptográfico.

EN.III.10.6.01: Verificar se a documentação especifica o código-fonte com comentários que esclareçam a correspondência dos componentes do módulo criptográfico.

REQUISITO III.10.7: [FIPS 140-2, 4.10] Se o módulo criptográfico contém componentes de hardware, a documentação deve listar tais componentes, apresentando os esquemas elétricos e/ou a linguagem de baixo nível.

EN.III.10.7.01: Verificar se a documentação lista os componentes de hardware do módulo criptográfico, apresentando os esquemas elétricos e/ou a linguagem de baixo nível.

REQUISITO III.10.8: [FIPS 140-2, 4.10] A documentação deve descrever a especificação das portas externas e interfaces do módulo criptográfico e o propósito dessas interfaces.

EN.III.10.8.01: Verificar se a documentação especifica cada interface e porta externa do módulo criptográfico.

EN.III.10.8.02: Verificar se a documentação especifica o propósito de cada uma dessas interfaces externas.

REQUISITO III.10.9: [FIPS 140-2, 4.10] Todos os componentes do módulo criptográfico devem ser implementados por uma linguagem de alto nível, exceto se o uso de uma linguagem de baixo nível (ex.: Assembly) for tido como essencial em relação ao desempenho ou quando a linguagem de alto nível não estiver disponível.

EN.III.10.9.01: Identificar cada componente de software e hardware que não tiver sido escrito em linguagem de alto nível e verificar se a documentação justifica o motivo desses componentes terem sido escritos usando linguagem de baixo nível. A documentação pode citar a indisponibilidade da linguagem de alto nível ou a necessidade de ganho de performance para o software ou *firmware*.

2.1.13 Mitigações de ataques

REQUISITO III.11.1: A documentação técnica do módulo criptográfico deve especificar quais os tipos de ataques classificados como não invasivos são mitigados pelo módulo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.11.1.01: Verificar se a documentação técnica atende ao **REQUISITO III.11.1.**

REQUISITO III.11.2: A documentação técnica do módulo criptográfico deve especificar quais outros tipos de ataques são mitigados pelo módulo.
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.11.2.02: Verificar se a documentação técnica atende ao **REQUISITO III.11.2.**

RECOMENDAÇÃO III.11.1: É recomendável que módulos criptográficos possuam proteções contra ataques não invasivos, como por exemplo, ataques por meio de emanações eletromagnéticas (EMA).
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.11.1.01: Verificar se a documentação técnica descreve proteções do módulo criptográfico contra ataques não invasivos.

2.2 Requisitos de gerenciamento

Gerenciamento do **hardware**

2.2.1.1 Backup e recuperação

REQUISITO IV.1.1: O módulo criptográfico deve atender aos requisitos de *backup* e recuperação, conforme descrito nos itens a seguir.

- Operadores com papéis de oficial de segurança (SO), usuário ou usuário de manutenção devem ser capazes de invocar a função de *backup*;
- O sistema deverá prover a capacidade de *backup* do conteúdo criptográfico sem comprometer a confidencialidade e integridade deste;
- O sistema de *backup* e recuperação deve estar cifrado para não comprometer a segurança;

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.1.1.01: Verificar se a documentação especifica os itens do **REQUISITO IV.1.1**.

EN.IV.1.1.02: Verificar se operadores com papéis de oficial de segurança (SO), usuário ou usuário de manutenção são capazes de invocar a função de *backup.*

EN.IV.1.1.03: Verificar se o sistema provê a capacidade de *backup* do conteúdo criptográfico e se este mantém a confidencialidade e integridade.

EN.IV.1.1.04: Verificar se o sistema de *backup* e recuperação é cifrado para não comprometer a segurança.

2.2.1.2 Proteção contra falhas

REQUISITO IV.1.2: O sistema deve oferecer mecanismos de proteção contra falhas originadas por falta de energia e falhas de comunicação. Após uma falha ou descontinuidade do serviço, o equipamento deve entrar em modo não operacional, e quando terminado, deve ser colocado em estado de operação segura;
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.1.2.01: Verificar se a documentação especifica o **REQUISITO IV.1.2**.

EN.IV.1.2.02: Verificar se o sistema oferece mecanismos de proteção contra falhas originadas por falta de energia e falhas de comunicação.

EN.IV.1.2.03: Provocar uma falha ou descontinuidade do serviço e verificar se o equipamento entra em modo de manutenção (se esse modo estiver ativo), e quando terminado, verificar se é colocado em estado de operação segura.

2.2.1.3 Atualização e integridade do firmware

REQUISITO IV.1.3: A integridade do *firmware* deverá ser garantida por mecanismo de detecção de alteração indevida, podendo ser baseado em função de hash ou equivalente. A integridade deverá ser checada quando o *firmware* é carregado, atualizado e toda vez que o hardware (MSC) é ativado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.1.3.01: Verificar se a documentação especifica um mecanismo de detecção de alteração indevida baseado em função de *hash* ou equivalente.

EN.IV.1.3.02: Carregue o *firmware* e verifique a sua integridade através do mecanismo de detecção de alteração indevida, baseado em função de *hash* ou equivalente.

2.2.1.4 Controle de ativação com segredo compartilhado M de N (sistema Shamir Secret Sharing)

REQUISITO IV.1.4: O hardware (MSC) deverá dispor de mecanismo de ativação por segredo compartilhado M de N, que provê a capacidade de implementar uma política de divisões de responsabilidades e integridade multi-pessoal na ativação deste.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.1.4.01: Verificar se a documentação especifica mecanismo de ativação por segredo compartilhado M de N.

EN.IV.1.4.02: Executar o sistema para inserir N operadores com papéis de oficial de segurança (SO), usuários ou usuários de manutenção. Entrar no sistema e verificar se é possível ativá-lo com M dos N operadores com papéis de oficial de segurança (SO), usuários ou usuários de manutenção inseridos anteriormente.

2.2.1.5 Utilitários de administração e diagnósticos

RECOMENDAÇÃO IV.1.1: Se o fabricante dispor de utilitários de gerenciamento e diagnósticos de problemas, então deve disponibilizar documentação detalhada sobre esses utilitários disponíveis para operadores com níveis de administrador e usuário.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.IV.1.1.01: Verificar se a documentação especifica utilitários de gerenciamento e diagnósticos de problemas.

EN.REC.IV.1.1.02: Verificar se a documentação detalha cada um desses utilitários disponíveis para operadores com níveis de administrador e usuário.

2.2.2 Gerenciamento do módulo criptográfico

REQUISITO IV.2.1: O módulo criptográfico deve atender aos requisitos de gerenciamento ora estabelecidos, conforme descrito nos itens a seguir.
Nota: Este requisito é testado como parte do **REQUISITO IV.2.2.**

REQUISITO IV.2.2: Funcionalidades de gerenciamento do módulo criptográfico devem estar disponíveis ao operador por meio de uma ferramenta específica ou utilitário. Tal utilitário deve ser provido pelo fornecedor do módulo criptográfico contendo, no mínimo, mas não limitado, os seguintes aspectos:

- Possuir interface gráfica nos idiomas: português do Brasil ou inglês;
- Permitir importação e exportação de chaves criptográficas simétricas ou assimétricas;
- Permitir ao operador apagar chaves criptográficas e outros dados contidos no módulo criptográfico, segundo os procedimentos adequados de autenticação, caso seja necessário;
- Permitir ao operador a troca do mecanismo de autenticação;
- Permitir a reinicialização dos módulos criptográficos.

Procedimentos de ensaio para NSH 1:

EN.IV.2.2.01: Analisar se a documentação descreve os itens do **REQUISITO IV.2.2.**

Nota: Os ensaios referentes a esta seção serão realizados por meio de uma ferramenta ou utilitário provido pelo fornecedor do módulo, com base nas APIs e nas plataformas de sistemas operacionais definidas no Manual de Condutas Técnicas 7 - Volume I.

EN.IV.2.2.02: Verificar se o utilitário possui interface gráfica nos idiomas: português do Brasil ou inglês.

EN.IV.2.2.03: Importar chaves criptográficas simétricas. Após a importação, verificar se a chave importada está presente no módulo criptográfico e executar operações criptográficas que validem essas chaves.

EN.IV.2.2.04: Importar chaves criptográficas assimétricas. Após a importação, verificar se a chave importada está presente no módulo criptográfico e executar operações criptográficas que validem essas chaves.

EN.IV.2.2.05: Exportar chaves criptográficas simétricas. Após a exportação, executar operações criptográficas que validem essas chaves.

EN.IV.2.2.06: Exportar chaves criptográficas assimétricas. Após a exportação, executar operações criptográficas que validem essas chaves.

EN.IV.2.2.07: Verificar se é possível apagar chaves criptográficas e outros dados contidos no módulo criptográfico, através de procedimentos adequados de autenticação.

EN.IV.2.2.08: Verificar se é possível um operador trocar o meio de autenticação.

EN.IV.2.2.09: Verificar se é possível reinicializar o módulo criptográfico.

2.2.3 Gerenciamento de chaves criptográficas

REQUISITO IV.3.1: Os seguintes requisitos funcionais de gerenciamento de chaves criptográficas devem estar disponíveis por invocação via API ou via ferramenta de administração do MSC para avaliação dos algoritmos criptográficos quando não se dispõe de código-fonte para análise:

- Gerar chave criptográfica assimétrica de forma aleatória no módulo criptográfico;

- Gerar chave criptográfica assimétrica de forma conhecida no módulo criptográfico;
- Gerar chave criptográfica simétrica de forma aleatória no módulo criptográfico;
- Gerar chave criptográfica simétrica de forma conhecida no módulo criptográfico;
- Apagar chave criptográfica assimétrica com sobrescrita de valores;
- Apagar chave criptográfica simétrica com sobrescrita de valores;
- Recuperar parâmetros sobre uma determinada chave criptográfica simétrica, tais como:
    - Algoritmo;
    - Tamanho da chave;
    - Valor;
    - Permissões.
- Recuperar parâmetros sobre uma determinada chave criptográfica assimétrica, tais como:
    - Algoritmo;
    - Expoente público (RSA);
    - Módulo (RSA);
    - Tamanho da chave;
    - Permissões.

Procedimentos de ensaio para NSH 1:

EN.IV3.1.01: Analisar se a documentação descreve os requisitos de gerenciamento de chaves criptográficas.

Nota: Os ensaios referentes a esta seção serão realizados por meio de uma ferramenta ou utilitário provido pelo fornecedor do módulo, baseando-se nas APIs e nas plataformas de sistemas operacionais definidas no Manual de Condutas Técnicas 7 - Volume I.

EN.IV.3.1.02: 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 essas chaves assimétricas.

EN.IV.3.1.03: Gerar chaves criptográficas assimétricas de forma conhecida no módulo criptográfico. Após a geração, verificar se a chave gerada está presente no módulo criptográfico e executar operações criptográficas que validem essas chaves assimétricas.

EN.IV.3.1.04: Gerar chaves criptográficas simétricas 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 essas chaves simétricas.

EN.IV.3.1.05: Gerar chaves criptográficas simétricas de forma conhecida no módulo criptográfico. Após a geração, verificar se a chave gerada está presente no módulo criptográfico e executar operações criptográficas que validem essas chaves simétricas.

EN.IV.3.1.06: Escolher uma determinada chave criptográfica simétrica e depois recuperar seus parâmetros associados. Após a recuperação, verificar se os parâmetros obtidos correspondem à chave selecionada.

EN.IV.3.1.07: Escolher uma determinada chave criptográfica assimétrica e depois recuperar seus parâmetros associados. Após a recuperação, verificar se os parâmetros obtidos correspondem à chave selecionada.

Procedimentos de ensaio para NSH 2 e 3:

EN.IV.3.1.08: Verificar, por meio de inspeção direta do código-fonte do módulo criptográfico, se a destruição de chaves criptográficas assimétricas é realizada por meio da técnica de sobrescrita de valores.

EN.IV.3.1.09: Verificar, por meio de inspeção direta do código-fonte do módulo criptográfico, se a destruição de chaves criptográficas simétricas é realizada por meio da técnica de sobrescrita de valores.

2.2.4 Exportação e importação

REQUISITO IV.4.1: Os seguintes requisitos funcionais de exportação e importação devem estar disponíveis por invocação via API ou via ferramenta de administração do MSC:

- Exportar chave criptográfica assimétrica pública do módulo criptográfico; A exportação de chave criptográfica assimétrica privada só é válida para certificados dos tipos A1, A2, S1 e S2;
- Gerar cópia de segurança da chave criptográfica assimétrica privada do módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.4.1.01: Analisar se a documentação descreve os requisitos de exportação e importação.

Nota: Os ensaios referentes a esta seção serão realizados por meio de uma ferramenta ou utilitário provido pelo fornecedor do módulo, com base nas APIs e nas plataformas de sistemas operacionais definidas no Manual de Condutas Técnicas 7 - Volume I.

EN.IV.4.1.02: Exportar a 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.4.1.03: Gerar cópia de segurança da chave criptográfica assimétrica privada do módulo criptográfico. Após a geração, verificar se a chave foi gerada e executar operações criptográficas que validem a chave.

2.3 Requisitos de interoperabilidade

Os requisitos de interoperabilidade 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*) numa maneira que garanta um conjunto mínimo de funcionalidades ou por meio de ferramenta de administração.

2.3.1 Requisitos gerais de interoperabilidade

REQUISITO V.1.1: No mínimo uma das seguintes APIs serão consideradas para análise dos requisitos de interoperabilidade:

- Microsoft CryptoAPI;
- PKCS#11 v. 2.11;
- JCE/JCA;
- Interface própria;
- OpenSSL Engine.

Nota: Este requisito não é testado separadamente e faz parte da s**eção 5.1.**

REQUISITO V.1.2: Quando aplicável e possível, nos componentes de software da arquitetura do módulo criptográfico, os requisitos funcionais devem estar disponíveis por invocação, via API, nas seguintes plataformas de sistemas operacionais:

a. Linux kernel 2.4 e versões superiores;
b. Microsoft Windows 2000 e versões superiores.

Nota: Este requisito não é testado separadamente e faz parte da s**eção 5.1.**

2.3.1.1 Requisitos gerais

REQUISITO V.1.3: Para avaliação dos algoritmos quando não se dispõe de código-fonte para análise, o módulo criptográfico deve ser capaz de executar as seguintes operações:

- Gerar chaves simétricas especificando os componentes de chaves simétricas em texto claro;

- Gerar par de chaves especificando os componentes de chaves assimétricas em texto claro. Por exemplo os componentes Módulo, Expoente público, tamanho em bits, etc;
- Gerar objeto de chaves especificando os componentes de chaves assimétricas (no mínimo chave pública) em texto claro. Por exemplo os componentes: Módulo, Expoente público, Expoente Privada em forma reduzida ou em forma de TRC (Teorema de Resto Chinês);
- Cifrar e decifrar chaves especificando os componentes de chaves simétricas ou assimétrica em texto claro;
- Importar chaves (PKCS#12) especificando os componentes de chaves assimétricas privadas criptografados;
- Assinar conteúdo especificando os componentes de chaves assimétricas públicas em texto claro;
- Verificar assinatura especificando os componentes de chaves assimétricas públicas em texto claro.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.3.01: Analisar se a documentação corresponde aos requisitos gerais do módulo criptográfico.

Nota: Os ensaios referentes a esta seção serão realizados por meio de uma ferramenta ou utilitário provido pelo fornecedor do módulo, com base nas APIs e nas plataformas de sistemas operacionais.

EN.V.1.3.02: Gerar par de chaves assimétricas especificando os componentes das chaves em texto claro. Após a geração, verificar se as chaves foram geradas, se os componentes das chaves estão em texto claro e executar operações criptográficas que validem as chaves.

EN.V.1.3.03: Cifrar e decifrar chaves assimétricas especificando os componentes das chaves em texto claro. Após cifrar/decifrar as chaves, verificar se as operações foram geradas, se os componentes das chaves estão em texto claro e executar operações criptográficas que validem as chaves.

EN.V.1.3.04: Importar chaves assimétricas especificando os componentes de chaves assimétricas privadas criptografados. Após importar as chaves, verificar se as operações foram realizadas, se os componentes da chave pública estão em texto claro, se os da chave privada estão criptografados e executar operações criptográficas que validem as chaves.

EN.V.1.3.05: Assinar conteúdo especificando os componentes das chaves assimétricas públicas em texto claro. Após a assinatura, verificar se a mesma foi gerada corretamente, se os componentes das chaves assimétricas públicas estão em texto claro e executar operações criptográficas que validem a operação.

EN.V.1.3.06: Verificar uma assinatura especificando os componentes de chaves assimétricas públicas em texto claro. Após a verificação, verificar se os componentes das chaves assimétricas públicas estão em texto claro e executar operações criptográficas que validem a operação.

REQUISITO V.1.4: A implementação da interface proprietária deve suportar os algoritmos criptográficos descritos na seção 3.1.1, "Algoritmos Criptográficos Obrigatórios".

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.4.01: Verificar se a documentação que acompanha o módulo criptográfico especifica o suporte aos algoritmos criptográficos descritos na seção 3.1.1 "Algoritmos criptográficos obrigatórios".

2.3.1.2 Requisitos sobre CryptoAPI

REQUISITO V.1.5: O módulo criptográfico deve suportar, no mínimo, uma implementação do MS CryptoAPI, versão 1.0.
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.5.01: Verificar na documentação se o CSP suporta uma implementação do MS CryptoAPI.

REQUISITO V.1.6: O módulo criptográfico deve exportar, isto é, expor sua interface, das seguintes chamadas:

- *CryptAcquireContext*
- *CryptCreateHash*
- *CryptDecrypt*
- *CryptDeriveKey*
- *CryptDestroyHash*
- *CryptDestroyKey*
- *CryptEncrypt*
- *CryptExportKey*
- *CryptGenKey*
- *CryptGenRandom*
- *CryptGetHashParam*
- *CryptGetKeyParam*
- *CryptGetProvParam*
- *CryptGetUserKey*
- *CryptHashData*
- *CryptHashSessionKey*
- *CryptImportKey*
- *CryptReleaseContext*
- *CryptSetHashParam*
- *CryptSetKeyParam*
- *CryptSetProvParam*
- *CryptSignHash*
- *CryptVerifySignature*

Sendo obrigatória a implementação das seguintes funções:

- *CryptAcquireContext* para criação de chaves assimétricas e remoção de *key containers* existentes.
- *CryptGenKey* tanto para chaves simétricas quanto para assimétricas;
- *CryptImportKey* especificando tanto as chaves simétricas quanto as assimétricas;

- *CryptGetKeyParam* para recuperação de parâmetros de permissões de acesso às chaves criadas/existentes em um *key container*;
- *CryptHashData e CryptSignHash* para geração de assinatura utilizando chave assimétrica;
- *CryptVerifySignature* para verificação da assinatura após a importação da chave pública via *CryptImportKey.*

As funções não implementadas devem retornar o código de erro *E_NOTIMPL*.

Procedimentos de ensaio para NSH 1:

EN.V.1.6.01: Verificar na documentação se o módulo criptográfico exporta as chamadas citadas no requisito.

EN.V.1.6.02: Verificar na documentação se o módulo criptográfico implementa as chamadas tidas como obrigatórias.

Procedimentos de ensaio para NSH 2 e 3:

EN.V.1.6.03: Verificar na implementação das funções do módulo criptográfico, se as funções do MS CryptoAPI não implementadas retornam o código de erro E_NOTIMPL.

REQUISITO V.1.7: A implementação de MS CryptoAPI deve suportar os algoritmos criptográficos descritos na seção 3.1.1, "Algoritmos Criptográficos Obrigatórios".
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.7.01: Verificar se a documentação que acompanha o módulo criptográfico especifica o suporte aos algoritmos criptográficos descritos na seção "Algoritmos Criptográficos Obrigatórios" por meio de interface MS CryptoAPI.

2.3.1.3 Requisitos sobre PKCS#11

REQUISITO V.1.8: O módulo criptográfico deve suportar uma implementação PKCS#11 na versão no mínimo 2.11.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.8.01: Verificar na documentação se o módulo criptográfico suporta uma implementação PKCS#11.

EN.V.1.8.02: Verificar se a documentação que acompanha o módulo criptográfico especifica a versão do PKCS#11 suportado.

REQUISITO V.1.9: O módulo criptográfico deve suportar as seguintes chamadas de PKCS#11 (Cryptoki):

- *C_Initalize*
- *C_Finalize*
- *C_OpenSession*
- *C_CloseSession*
- *C_Init_Token*
- *C_Init_PIN*
- *C_Login*
- *C_Logout*
- *C_CreateObject*
- *C_DestroyObject*
- *C_GetAttributeValue*
- *C_SetAttributeValue*
- *C_EncryptInit*
- *C_Encrypt*
- *C_DecryptInit*
- *C_Decrypt*
- *C_DigestInit*

- *C_Digest*
- *C_DigestKey*
- *C_SignInit*
- *C_Sign*
- *C_VerifyInit*
- *C_Verify*
- *C_GenerateKey*
- *C_GenerateKeyPair*
- *C_DeriveKey*
- *C_GenerateRandom*

Sendo obrigatória a implementação das seguintes funções:

- *C_GenerateKey* especificando templates de chaves simétricas;
- *C_GenerateKeyPair* especificando templates de chaves assimétricas;
- *C_Sign* para realizar assinatura de um conteúdo;
- *C_Verify* para verificar a assinatura de um conteúdo;
- *C_Encrypt* para cifrar um dado com uma chave já construída;
- *C_Decrypt* para decifrar um dado com uma chave já construída;
- *C_CreateObject* especificando templates de chaves assimétricas (no mínimo chave pública);
- *C_DestroyObject* especificando o *handle* do objeto.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.9.01: Verificar na documentação se o módulo criptográfico exporta as chamadas citadas no requisito.

EN.V.1.9.02: Verificar na documentação se o módulo criptográfico implementa as funções tidas como obrigatórias.

REQUISITO V.1.10: A implementação PKCS#11 deve suportar os algoritmos criptográficos descritos na seção 3.1.1, "Algoritmos Criptográficos Obrigatórios".

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.10.01: Verificar se a documentação que acompanha o módulo criptográfico especifica o suporte aos algoritmos criptográficos descritos na seção "Algoritmos criptográficos obrigatórios" por meio de interface PKCS#11.

2.3.1.4 Requisitos sobre Java Cryptographic Extension (JCE)

REQUISITO V.1.11: O pacote de classes JCE deve ser suportado pela versão da máquina virtual Java 1.4.2 ou superior.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.11.01: Verificar na documentação se o módulo criptográfico suporta uma implementação JCE.

EN.V.1.11.02: Verificar se a documentação que acompanha o módulo criptográfico especifica a versão da máquina virtual Java a ser suportada pelo pacote de classes JCE.

REQUISITO V.1.12: O módulo criptográfico deve suportar, no mínimo, as seguintes classes de JCE [Java 2 SDK]:

- *MessageDigest*
- *Signature*
- *KeyPairGenerator*
- *KeyFactory*
- *CertificateFactory*
- *KeyStore*
- *AlgorithmParameters*
- *AlgorithmParameterGenerator*
- *SecureRandom*

- *CertPathBuilder*
- *CertPathValidator*
- *CertStore*

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.12.01: Verificar na documentação se o módulo criptográfico suporta as classes JCE tidas como obrigatórias.

REQUISITO V.1.13: A documentação deve especificar os componentes de software implementados do provedor de serviço criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.13.01: Verificar se a documentação que acompanha o módulo criptográfico especifica os componentes de software implementados do provedor de serviço criptográfico, de acordo com o documento de especificação da API *Java Cryptography Architecture API Specification & Reference*.

REQUISITO V.1.14: A documentação deve especificar o processo de configuração e instalação do provedor de serviço criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.14.01: Verificar se a documentação que acompanha o módulo criptográfico especifica o processo de configuração e instalação do módulo criptográfico na máquina virtual Java.

REQUISITO V.1.15: A documentação deve especificar serviços criptográficos implementados no provedor de serviço criptográfico que não estejam na especificação JCE versão 1.4 ou superior.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.15.01: Verificar se a documentação que acompanha o módulo criptográfico especifica os serviços criptográficos implementados no módulo criptográfico que não estejam na especificação JCE versão 1.4 ou superior.

REQUISITO V.1.16: A documentação deve informar detalhes sobre o uso do provedor de serviço criptográfico como API no formato Javadoc com trechos de código-fonte.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.16.01: Verificar se a documentação que acompanha o módulo criptográfico informa detalhes sobre o uso do módulo criptográfico como API no formato Javadoc com trechos de código-fonte.

REQUISITO V.1.17: A implementação JCE deve suportar os algoritmos criptográficos descritos na seção 2.1.1, "Algoritmos Criptográficos Obrigatórios".

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.17.01: Verificar se a documentação que acompanha o módulo criptográfico especifica o suporte aos algoritmos criptográficos descritos na seção "Algoritmos criptográficos obrigatórios" por meio de interface JCE.

RECOMENDAÇÃO V.1.1: Se aplicável, o provedor de serviço criptográfico será assinado por uma chave privada ligada a um certificado digital reconhecido no âmbito ICP-Brasil.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.V.1.1.01: Verificar na documentação que acompanha o módulo criptográfico se o módulo criptográfico é assinado por uma chave privada ligada a um certificado digital reconhecido no âmbito ICP-Brasil.

2.3.1.5 Requisitos sobre OpenSSL

OBSERVAÇÃO: Requisitos sobre OpenSSL devem ser avaliados apenas se esta API for implementada.

Nota: Os ensaios referentes a esta seção serão realizados por meio de uma ferramenta de software ou utilitário, com base nas APIs e nas plataformas de sistemas operacionais.

REQUISITO V.1.18: O CSP deve ser capaz de implementar as seguintes rotinas do OpenSSL Engine:

- *ENGINE_init;*
- *ENGINE_finish;*
- *bind_fn;*
- *Engine_load;*
- *ENGINE_load_private_key;*
- *ENGINE_load_public_key;*
- *bind_helper;*
- *ENGINE_destroy;*
- Dentre as funções requeridas para operações RSA estão (RSA_METHOD):
    - *RSA_init;*
    - *RSA_finish;*
    - *RSA_pub_dec ou RSA_verify (1);*
    - *RSA_priv_enc ou RSA_sign (1);*
    - *RSA_pub_enc;*
    - *RSA_priv_dec;*

    OBS: (1) Por questão de compatibilidade o OpenSSL ainda mantém as duas funções, tendo um campo para setar um flag (RSA_FLAG_SIGN_VER) de que versão é suportada.
- Funções requeridas para geração de números aleatórios (RAND_METHOD):
    - *RAND_bytes;*
    - *RAND_pseudo_bytes;*

- *RAND_status.*

Procedimentos de ensaio para NSH 1:

EN.V.1.18.01: Analisar se a documentação e verificar se foram implementadas as rotinas do OpenSSL Engine tidos como obrigatórios.

Procedimentos de ensaio para NSH 2 e 3:

EN.V.1.18.02: Verificar se as funções e definições do OpenSSL Engine tidas como obrigatórias para um OpenSSL Engine estão operacionais.

REQUISITO V.1.19: A implementação da API "Engine" OpenSSL deve suportar os algoritmos criptográficos descritos na seção 3.1.1, "Algoritmos Criptográficos Obrigatórios".

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.1.19.01: Verificar se a documentação que acompanha o módulo criptográfico especifica o suporte aos algoritmos criptográficos descritos na seção "Algoritmos criptográficos obrigatórios" por meio de interface OpenSSl Engine.

2.3.2 Requisitos de armazenamento

REQUISITO V.2.1: O módulo criptográfico deve possuir capacidade de armazenamento de, no mínimo, 32 Kbytes.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.2.1.01: Analisar se a documentação descreve a capacidade de armazenamento do módulo criptográfico reservada para certificados digitais.

EN.V.2.1.02: Por meio de ferramenta específica (por exemplo, utilitário de gerenciamento), gravar certificados digitais de tamanhos conhecidos na área de armazenamento do módulo criptográfico, totalizando um volume de dados escritos maior que 32 Kbytes. Após a gravação, verificar que foi possível a gravação de, pelo menos, 32 Kbytes de memória contendo certificados digitais na área de armazenamento do módulo.

REQUISITO V.2.2: Deve ser possível por meio de um dos APIs listados na seção 5.1 chamar funções que retornam a capacidade de armazenamento do módulo criptográfico.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.V.2.2.01: Analisar a documentação e verificar se um dos APIs listados na seção 5.1 possui funções que retornem a capacidade de armazenamento do módulo criptográfico.
Nota: Os ensaios referentes a este requisito serão realizados por meio de uma ferramenta de software ou utilitário, com base nas APIs e nas plataformas de sistemas operacionais.

EN.V.2.2.02: Chamar essas funções e verificar se as mesmas retornam a capacidade de armazenamento do módulo criptográfico.

2.4 Requisitos para restrição de substâncias nocivas

RECOMENDAÇÃO VI.1: É recomendável que o equipamento esteja em conformidade com as regras da Diretiva da União Européia (2002/95/EC) de Restrição às Substâncias Nocivas (RoHS – *Restriction to the use of Hazardous Substances*), respeitando as restrições impostas às substâncias citadas.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.VI.1.01: Analisar e verificar se a documentação especifica a conformidade do equipamento à Diretiva RoHS, respeitando as restrições impostas às substâncias citadas.

RECOMENDAÇÃO VI.2: É recomendado à parte interessada entregar documentação detalhando a conformidade do equipamento e de suas partes (materiais, peças, componentes, etc) com as diretrizes da RoHS, especificando a concentração das substâncias presentes dentro da proporção sugerida pela convenção RoHS:

- Chumbo (Pb) – Valor de Concentração Máxima – 1000 ppm, ou 100 mg / Kg de material homogêneo;
- Mercúrio (Hg) – Valor de Concentração Máxima – 1000 ppm, ou 100 mg / Kg de material homogêneo;
- Cromo Hexavalente ou Cromo VI (Cr(VI)) – Valor de Concentração Máxima –1000 ppm, ou 100 mg / Kg de material homogêneo;
- Cádmio (Cd) – Valor de Concentração Máxima – 100 ppm, ou 100 mg / Kg de material homogêneo;
- Bromobifenilas (PBB) – Valor de Concentração Máxima – 1000 ppm, ou 100 mg / Kg de material homogêneo;
- Éteres de Bromobifenilas (PBDE) – Valor de Concentração Máxima – 1000 ppm, ou 100 mg / Kg de material homogêneo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.VI.2.01: Analisar e verificar se a documentação indica a concentração das substâncias presentes no equipamento e suas partes (materiais, peças, componentes, etc) dentro dos padrões sugeridos pela Diretiva RoHS.

RECOMENDAÇÃO VI.3: É recomendado à parte interessada apresentar certificado dos fornecedores de materiais, peças, componentes ou partes integrantes do equipamento final atestando a conformidade com a diretiva da RoHS.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.VI.3.01: Analisar e verificar se a documentação apresenta certificados dos fornecedores de materiais, peças, componentes ou partes integrantes do equipamento final atestando a conformidade à Diretiva RoHS.

2.5 Requisitos de documentação

REQUISITO VII.1: A parte interessada (PI) deve fornecer manual de instalação, especificando a arquitetura da máquina na qual é suportada a instalação do MSC.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.1.01: Analisar a documentação e verificar se o manual de instalação especifica corretamente o processo de instalação do MSC que está sendo homologado.

REQUISITO VII.2: A PI deve fornecer o manual de instalação, especificando os sistemas operacionais suportados pelo MSC.
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.2.01: Analisar a documentação e verificar se o manual de instalação especifica quais componentes de software serão necessários para a ativação do MSC, tais como, JVM e sistema operacional compatíveis.

REQUISITO VII.3: A PI deve fornecer o manual de configuração, detalhando as ferramentas e recursos disponíveis para a configuração do MSC na máquina onde o mesmo será implantado.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.3.01: Analisar a documentação e verificar se o manual de configuração especifica corretamente o processo para configurar o MSC que está sendo homologado.

EN.VII.3.02: Analisar a documentação e verificar se o manual de configuração especifica quais procedimentos de inicialização devem ser adotados previamente a sua ativação.

EN.VII.3.03: Analisar a documentação e verificar se o manual de configuração especifica os procedimentos que devem ser adotados para habilitação do MSC na arquitetura criptográfica.

REQUISITO VII.4: A PI deve fornecer o manual de operador, detalhando as ferramentas e recursos disponíveis aos operadores do MSC.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.4.01: Analisar a documentação e verificar se o manual do operador detalha corretamente as ferramentas e recursos disponíveis do MSC que está sendo homologado.

EN.VII.4.02: Analisar a documentação e verificar se o manual do operador especifica a versão e configuração de acesso do MSC.

REQUISITO VII.5: A PI deve fornecer o manual de administrador (*Security Officer)*, detalhando as ferramentas e recursos disponíveis somente aos administradores do MSC.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.5.01: Analisar a documentação e verificar se o manual do administrador detalha corretamente as ferramentas e recursos disponíveis do MSC que está sendo homologado.

EN.VII.5.02: Analisar a documentação e verificar se o manual do administrador especifica quais interfaces de administração e/ou configuração estão disponíveis, como por exemplo, arquivos-texto de configuração.

EN.VII.5.03: Analisar a documentação e verificar se o manual do administrador especifica a versão e configuração de acesso do MSC.

REQUISITO VII.6: A PI deve fornecer o manual de desenvolvedor detalhando eventualmente a(s) API(s) proprietária(s) para desenvolvimento de aplicações utilizando o MSC caso exista.
Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.6.01: Analisar a documentação e verificar se o manual do desenvolvedor especifica corretamente as funções da API do MSC que está sendo homologado.

EN.VII.6.02: Analisar a documentação e verificar se o manual do desenvolvedor especifica a arquitetura do sistema.

EN.VII.6.03: Analisar a documentação e verificar se o manual do desenvolvedor especifica as APIs implementadas na arquitetura criptográfica.

EN.VII.6.04: Analisar a documentação e verificar se o manual do desenvolvedor especifica os tratamentos de erros das chamadas das funções da API.

REQUISITO VII.7: A PI deve fornecer o manual de integração do MSC com a(s) API(s) de mercado para desenvolvimento de sistemas integrados.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.7.01: Analisar a documentação e verificar se o manual de integração especifica corretamente as integrações das funções da API do MSC que está sendo homologado com as APIs de mercado para desenvolvimento de sistemas integrados.

REQUISITO VII.8: A PI deve fornecer manual de importação de chaves para dentro do MSC, detalhando a aplicabilidade do uso de outros hardwares externos ao MSC.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.VII.8.01: Analisar a documentação e verificar se o manual de importação de chaves para dentro do MSC, detalha a aplicabilidade do uso de outros hardwares externos ao MSC.

3 Referências normativas

[1] [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 versão 2.1. Brasília. ICP-Brasil: 2007

[2] [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 ICP-Brasil.** DOC-ICP-10.02 versão 2.0. Brasília. ICP-Brasil: 2007

[3] [IN 05/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 05/2007: Padrões e procedimentos técnicos a serem observados nos processos de homologação de módulos de segurança criptográfica (MSC) no âmbito da ICP-Brasil.** DOC-ICP-10.05 versão 1.0. Brasília. ICP-Brasil: 2007

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

[5] [ANSI X9.17] AMERICAN NATIONAL STANDARDS INSTITUTE. **Key Management.** Descontinuado, mas o gerador de números pseudo-aleatórios baseado em cifra de bloco ainda é válido.

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

[7] [ANSI. X9.80] AMERICAN NATIONAL STANDARDS INSTITUTE. **Prime Number Generation, Primality Testing, and Primality Certificates.** 2005.

[8] [ANSI. X9.81-1] AMERICAN NATIONAL STANDARDS INSTITUTE. **Random Number Generation Part 1: Overview and Basic Principles.**

[9] [ANSI. X9.82-1] AMERICAN NATIONAL STANDARDS INSTITUTE. **Random Number Generation Part 1: Overview and Basic Principles.** 2006.

[10][CALIFORNIA ROHS WORKSHOP] CALIFORNIA EPA DEPARTMENT OF TOXIC SUBSTANCES CONTROL. **Hazardous waste management program: regulatory and program development division.**

[11] COMITÊ GESTOR DA ICP-BRASIL. **DOC ICP-01.01: Padrões e Algoritmos Criptográficos da Infra-estrutura de Chaves Públicas Brasileira (ICP-BRASIL).** Brasília. ICP-BRASIL: 2006.

[12]COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 38, de 18 de abril de 2006: Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil.** Brasília. ICP-BRASIL: 2006.

[13] COMITÊ GESTOR DA ICP-BRASIL. **Resolução N° 41, de 18 de abril de 2006: Requisitos Mínimos para as Políticas de Certificados na Infra-estrutura de Chaves Públicas Brasileira (ICP-BRASIL).** Brasília. ICP-BRASIL: 2006.

[14] **Cryptography (Windows) – MSDN (Microsoft Developer Network).** Disponível em: <http://msdn2.microsoft.com/en-us/library/aa380255.aspx>. Acesso em: 20.jul.2007.

[15] [EUROPEAN PARLIAMENT] **Directive 2002/95/ec of the European Parliament and of the Council on the Restriction of the use of certain hazardous substances in electrical and electronic equipment**. 2002.

[16] [EUROPEAN PARLIAMENT] **Frequently asked questions on hazardous substances in electrical and electronic equipment (rohs) and directive 2002/96/ec waste electrical and eletronic equipment directive (weee).** 2002.

[17] [FCC] CODE OF FEDERAL REGULATIONS 47 PART 15 - **Radio frequency devices - subpart b - unintentional radiators**. 2007.

[18] [IEC. CISPR 22] **Limits and methods of measurement of radio disturbance characteristics of ite**. 2006.

[19] [IEC. CISPR 24] **Limits and methods of measurement of the immunity characteristics of ite**. 1997.

[20] [IEC 60050 - 161] **International electrotechnical vocabulary**. 1990.

[21] [ISO/IEC 8825-1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).** Genève, Switzerland, Reference Number: ISO/IEC 8825-1:2002.

[22] [ITI] COMITÊ GESTOR DA ICP-BRASIL. **DOC ICP-01.01. Padrões e Algoritmos Criptográficos da Infra-Estrutura de Chaves Públicas Brasileira (ICP-BRASIL).** Versão 1.0. Brasília. ICP-BRASIL: 2006.

[23] [ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Manual de Condutas Técnicas 7 – Volume I**: **Requisitos Técnicos e Material de Depósito para Homologação de MSC.** Versão 1.0.

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

[25] **Java Cryptography Extension (JCE) for the Java 2 SDK,** versão 1.4. Disponível em: <http://java.sun.com/products/jce/index-14.html>. Acesso em 20.jul.2007.

[26] [NIST FIPS 197] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Advanced Encryption Standard (AES).** 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>. Acesso em: 20.jul.2007.

[27] [NIST / FIPS Special Publication 800-38C] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Counter with Cipher Block Chaining-Message Authentication Code (CCM).** 2004. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf>

[28] [NIST / FIPS 46-3] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Data Encryption Standard (DES)**. 1999. Disponível em: <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>. Acesso em: 20.jul.2007.

[29] [NIST. FIPS 140-2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules.** 2004.

[30] [NIST FIPS 186-2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Digital Signatura Standard (DSS).** 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>. Acesso em: 20.jul.2007.

[31] [NIST FIPS 196] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Entity Authentication Using Public Key Criptography.** 1997. Disponível em: <http://csrc.nist.gov/publications/fips/fips196/fips196.pdf>. Acesso em: 20.jul.2007.

[32] [NIST] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, [ITL] INFORMATION TECHNOLOGY LABORATORY. **Federal Information Processing Standards Publication – Security Requirements for**

Cryptographic Modules – FIPS PUB 140-2. Washington. US Government Printing Office: May 25, 2001.

[33] [NIST SP 800-17] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Modes of Operation Validation System (MOVS): Requirements and Procedures**, February 1998. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-17/800-17.pdf> Acesso em: 25 jul. 2005.

[34] [NIST SP 800-20] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS). Requirements and Procedures.** 2000. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-20/800-20.pdf> Acesso em: 25 jul. 2005.

[35] [NIST Special Publication 800-38B] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Recommendation for Block Cipher Modes of Operation - The CMAC Mode for Authentication.** 2005. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf>. Acesso em: 20.jul.2007.

[36] [NIST] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The Advanced Encryption Standard Algorithm Validation Suite (AESAVS).** 2002. 52 p. Disponível em: <http://csrc.nist.gov/cryptval/aes/AESAVS.pdf>. Acesso em: 25 jul. 2005.

[37] [NIST FIPS 198] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The Keyed-Hash Message Authentication Code (HMAC).** 2002. Disponível em: <http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf>. Acesso em: 20.jul.2007.

[38] [NIST] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The RSA Validation System (RSAVS).** 2004. Disponível em: <http://csrc.nist.gov/cryptval/dss/RSAVS.pdf>. Acesso em: 25 jul. 2005.

[39] [NIST FIPS 180-2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Secure Hash Standard (SHA).** 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>. Acesso em: 20.jul.2007.

[40] [NIST] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The Secure Hash Algorithm Validation System (SHAVS).** 2004. Disponível em: <http://csrc.nist.gov/cryptval/shs/SHAVS.pdf>. Acesso em: 25 jul. 2005.

[41] [NIST. FIPS 140-2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Security Requirements for Cryptographic Modules.** 2002.

[42] [NIST. FIPS 180-2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Secure Hash Standard (SHS) com nota de mudança 1.** 2004.

[43] [OpenSSL FIPS 1402] **Security Policy Object Module By the Open Source Software Institute** - Version 1.0a. March 24, 2006. Disponível em: <http://csrc.nist.gov/cryptval/140-1/140sp/140sp642.pdf>. Acesso em 20.jul.2007.

[44] [RSA LABORATORIES]. **CMS: Cryptographic Message Syntax Standard.** Version 1.5. 1993. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/ps/pkcs-7.ps>. Acesso em: 27.abril.2007.

[45] [RSA LABORATORIES] **PKCS#1: RSA Cryptography Standard.** Version 2.1. 2002. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf>. Acesso em: 30.noII.2006.

[46] [RSA LABORATORIES] **PKCS#5: Password-Based Cryptography Standard.** Version 2.0. 1999. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-5v2/pkcs5v2-0.pdf>. Acesso em: 30.noII.2006.

[47] [RSA LABORATORIES] **PKCS #10: Certification Request Syntax Standard** Version 1.7. 2000. 10p. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf>. Acesso em: 01.dez.2006.

[48] [RSA LABORATORIES] **PKCS#11: Cryptographic Token Interface Standard**. Version 2.0. 1997. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/pkcs11v2.pdf> Acesso em: 04.jul.2007.

[49] [SUN JCE] **Java Cryptography Extension (JCE) for the Java 2 SDK**, versão 1.4. Disponível em: <http://java.sun.com/products/jce/index-14.html>. Acesso em 20.jul.2007.

[50] THE INTERNET ENGINEERING TASK FORCE. Housley, R.; Polk, W.; Ford, W. e Solo, D. **Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.** RFC 3280, Category: Standards Track, April 2002. Disponível em <http://www.ietf.org/rfc/rfc3280.txt>. Acesso em: 30.jan.2006.

[51] THE INTERNET ENGINEERING TASK FORCE. Myers, M.; Ankney, R.; Malpani, A.; Galperin, S. e Adams, C. **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.** RFC 2560, Category: Standards Track, June 1999. Disponível em <http://www.ietf.org/rfc/rfc2560.txt>. Acesso em: 30.jan.2006.

[52] THE INTERNET ENGINEERING TASK FORCE. Housley, R. **Cryptographic Message Syntax (CMS).** RFC 3852, Category: Standards Track, July 2004. Disponível em <http://www.ietf.org/rfc/rfc3852.txt>. Acesso em: 30.jan.2006.

[53] THE INTERNET ENGINEERING TASK FORCE. Freed, N. e Borenstein, N. **Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies.** RFC 2045, Category: Standards Track, November 1996. Disponível em <http://www.ietf.org/rfc/rfc2045.txt>. Acesso em: 30.jan.2006.

[54] THE INTERNET ENGINEERING TASK FORCE. Linn, J. **Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures**. RFC 1421, February 1993. Disponível em: <http://www.ietf.org/rfc/rfc1421.txt>. Acesso em: 30.jan.2006.

ANEXO I

REQUISITOS PARA A AVALIAÇÃO DE MANUTENÇÃO

REQUISITO	Quantidade de ensaios
REQUISITO III.1.13	5
REQUISITO III.2.1	1
REQUISITO III.2.2	5
REQUISITO III.2.3	3
REQUISITO III.2.4	4
REQUISITO III.2.5	3
REQUISITO III.3.1	0
REQUISITO III.3.2	0
REQUISITO III.3.3	4
REQUISITO III.3.5	4
REQUISITO III.3.6	2
REQUISITO III.3.7	2
REQUISITO III.3.8	3
REQUISITO III.3.10	2
REQUISITO III.3.11	5
REQUISITO III.3.13	0
REQUISITO III.3.14	4
REQUISITO III.3.15	3
REQUISITO III.3.16	5
REQUISITO III.3.18	0
REQUISITO III.3.20	1
REQUISITO III.4.3	2
REQUISITO III.4.4	9
REQUISITO III.5.4	4
REQUISITO III.5.5	2

REQUISITO	Quantidade de ensaios
REQUISITO III.5.6	3
REQUISITO III.5.7	3
REQUISITO III.5.8	4
REQUISITO III.5.9	3
REQUISITO III.5.10	3
REQUISITO III.5.11	3
REQUISITO III.6.3	9
REQUISITO III.6.4	2
REQUISITO III.6.5	2
REQUISITO III.6.6	3
REQUISITO III.7.1	3
REQUISITO III.7.2	2
REQUISITO III.7.6	5
REQUISITO III.7.7	4
REQUISITO III.7.9	3
REQUISITO III.7.10	2
REQUISITO III.7.11	0
REQUISITO III.7.13	2
REQUISITO III.7.14	5
REQUISITO III.7.15	4
REQUISITO III.7.16	3
REQUISITO III.7.18	0
REQUISITO III.7.19	3
REQUISITO III.7.20	9
REQUISITO III.7.21	3
REQUISITO III.7.22.1	3
REQUISITO III.7.22.2	3
REQUISITO III.7.23	2
REQUISITO III.7.24	1
REQUISITO III.7.26	2
REQUISITO III.7.27	0
REQUISITO III.7.28	2

REQUISITO	Quantidade de ensaios
REQUISITO III.7.30	5
REQUISITO III.9.1	1
REQUISITO III.9.2	8
REQUISITO III.9.3	4
REQUISITO III.9.4	4
REQUISITO III.9.6	0
REQUISITO III.9.7	3
REQUISITO III.9.9	2
REQUISITO III.9.10	3
REQUISITO III.9.11	0
REQUISITO III.9.12	0
REQUISITO III.9.13	4
REQUISITO III.9.14	0
REQUISITO III.9.15	2
REQUISITO III.9.16	2
REQUISITO IV.1.1	4
REQUISITO IV.1.2	3
REQUISITO IV.1.3	2
REQUISITO IV.1.4	2
REQUISITO IV.3.1	9
REQUISITO IV.4.1	3
REQUISITO V.1.3	6