Infraestrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 7 – Volume I

Requisitos, Materiais e Documentos Técnicos para Homologação de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP-Brasil

Versão 2.2

Brasília, 26 de SETEMBRO de 2017

SUMÁRIO

CONTROLE DE ALTERAÇÕES....5
SIGLAS E ACRÔNIMOS....6
LISTAS DE ILUSTRAÇÕES....8
1 INTRODUÇÃO....9
1.1 Objetivo da homologação....9
1.2 Descrição do processo de homologação....9
1.3 Escopo do processo de homologação....10
1.4 Estruturação do MCT-7....11
2 PARTE 1....12
2.1 Requisitos Técnicos....13
2.1.1 Requisitos de especificação do módulo criptográfico....14
2.1.1.1 Algoritmos criptográficos obrigatórios....17
2.1.2 Portas e interfaces do módulo criptográfico....18
2.1.3 Papéis, serviços e autenticação....19
2.1.3.1 Papéis de acesso....20
2.1.3.2 Papel de acesso Usuário....21
2.1.3.3 Papel de acesso Oficial de Segurança (SO)....21
2.1.3.4 Papel de acesso Manutenção....22
2.1.3.5 Serviços....22
2.1.3.6 Autenticação de operadores do módulo criptográfico....23
2.1.4 Modelo de estado finito....26
2.1.5 Segurança Física....28
2.1.5.1 Requisitos gerais de segurança física....29
2.1.5.2 Requisitos específicos para proteção que evidencia violação....30
2.1.5.3 Requisitos específicos de proteção que resiste à violação....30
2.1.5.4 Requisitos específicos de proteção que detecta e responde à violação....31
2.1.6 Ambiente operacional....31
2.1.6.1 Ambiente operacional não modificável....32
2.1.6.2 Ambiente operacional modificável....32
2.1.7 Gerenciamento de chaves criptográficas....34
2.1.8 Geradores de números aleatórios....35

2.1.9 Geração de chaves criptográficas....36
2.1.9.1 Requisitos específicos de geração de chaves criptográficas....37
2.1.9.2 Importação e exportação de chaves criptográficas....37
2.1.9.3 Requisitos específicos de exportação de chaves criptográficas....38
2.1.9.4 Atribuição de chaves....39
2.1.9.5 Armazenamento de chaves criptográficas....40
2.1.9.6 Sobrescrita do valor de chaves criptográficas com zeros binários....40
2.1.10 Interferência/compatibilidade eletromagnética....41
2.1.11 Auto-testes....41
2.1.11.1 Testes de energização....42
2.1.11.2 Testes condicionais....43
2.1.12 Garantia de projeto....45
2.1.13 Mitigações de ataques....47
2.2 Requisitos de gerenciamento....47
2.2.1 Gerenciamento do hardware....48
2.2.1.1 Backup e recuperação....48
2.2.1.2 Proteção contra falhas....48
2.2.1.3 Atualização e integridade do firmware....48
2.2.1.4 Controle de ativação com segredo compartilhado M de N (sistema Shamir Secret Sharing)....48
2.2.1.5 Utilitários de administração e diagnósticos....49
2.2.2 Gerenciamento do módulo criptográfico....49
2.2.3 Gerenciamento de chaves criptográficas....50
2.2.4 Exportação e importação....50
2.3 Requisitos de interoperabilidade....51
2.3.1 Requisitos gerais de interoperabilidade....51
2.3.1.1 Requisitos gerais....51
2.3.1.2 Requisitos sobre CryptoAPI....52
2.3.1.3 Requisitos sobre PKCS#11....54
2.3.1.4 Requisitos sobre Java Cryptographic Extension (JCE)....55
2.3.1.5 Requisitos sobre OpenSSL....57
2.3.2 Requisitos de armazenamento....58

2.4 Requisitos para restrição de substâncias nocivas....58
2.5 Requisitos de documentação....59
3 PARTE 2....62
3.1 Depósito de materiais e documentos técnicos....63
3.2 Material e documentos técnicos a serem depositados....64
3.2.1 Componentes físicos....64
3.2.2 Documentos técnicos....65
3.2.3 Nível de Homologação 1....65
3.2.4 Manuais do produto....65
3.2.5 Documentação técnica específica....65
3.2.5.1 Documentação geral....71
3.2.6 Nível de Segurança da Homologação 2....71
3.2.7 Nível de Segurança da Homologação 3....72
3.3 Componentes em software executável....72
4 QUANTIDADES DE MATERIAIS E DOCUMENTOS TÉCNICOS A SEREM DEPOSITADOS....73
5 REFERÊNCIAS NORMATIVAS....77
ANEXO I....84

CONTROLE DE ALTERAÇÕES

Versão	Item Alterado	Descrição da Alteração
MCT 7 Vol. I Versão 2.2 IN 08, de 26/09/2017	1.3 e Anexo I	Previsão de autonomia para o OCP definir os ensaios nas Avaliações de Manutenção de Credenciamento.
MCT 7 Vol. I Versão 2.1	Índice	Numeração de itens para alinhar os volumes I e II
MCT 7 Vol. I Versão 2.0		Revisão do documento 08/11/2016
MCT 7 Vol. I Versão 1.0		Criação do documento 23/11/2007

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 Code*
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*
PRNG	*Pseudo Random Number Generator*
RNG	*Random Number Generators*

SIGLA	DESCRIÇÃO
RSA	*Rivest, Shamir and Adleman*
SDK	*Software Development Kits*
SHA	*Secure Hash Algorithm*
SO	Oficial de Segurança
SP	*Service Providers*
TDES	*Triple DES*

Listas de ilustrações

Lista de Figuras

Figura 1. Geradores de números aleatórios.....36

Lista de Tabelas

Tabela 1. Áreas de atuação do padrão FIPS 140-2.....13
Tabela 2. Quantidade de materiais e documentos técnicos a serem depositados.....75

1 Introdução

Este documento descreve os requisitos técnicos a serem observados no processo de 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.
Para uma melhor compreensão do disposto neste documento, corresponde ao módulo de segurança criptográfico:

- Um servidor ou placa auxiliar criptográfica fisicamente segura, resistente à violação que fornece funcionalidades criptográficas com capacidade de geração e armazenamento de chaves criptográficas simétricas e assimétricas voltados para utilização em uma Infraestrutura de Chaves Públicas (ICP).

Em módulos de segurança criptográficos, a fronteira criptográfica define um perímetro no qual estão contidos componentes tais como processador(es), memórias e outros dispositivos de hardware, software e *firmware.* A fronteira criptográfica também é delimitada por meio de mecanismos de segurança física para proteger estes componentes contra sondagem, observação e manipulação direta.
Neste documento, o termo "módulo criptográfico" será usado em referência a região contida pela fronteira criptográfica dentro do MSC.

1.1 Objetivo da homologação

O objetivo do processo de homologação do módulo de segurança criptográfico é propiciar a interoperabilidade e operação segura do serviço criptográfico ICP oferecido por um módulo de segurança criptográfico por meio da avaliação técnica de aderência aos requisitos técnicos definidos para este processo.

1.2 Descrição do processo de homologação

O processo de homologação é baseado em um conjunto de requisitos técnicos que devem ser atendidos por um módulo de segurança criptográfico para garantia da interoperabilidade e operação segura.
Estes requisitos técnicos são avaliados segundo ensaios de aderência aos requisitos técnicos. Para a realização dos ensaios, a parte interessada deve submeter ao processo de homologação um

conjunto de materiais requisitados, através de um procedimento denominado depósito de material.

1.3 Escopo do processo de homologação

Módulos de segurança criptográficos podem oferecer suporte a outros serviços ou subsistemas, coexistindo de forma integrada ou não com o ambiente ICP. Exemplos que podem ser citados são algoritmos financeiros (ex, verificação de PIN da VISA), controle de acesso físico (ex, PIV) e outros.

Assim, o escopo da avaliação considera o ambiente ICP, porém levando em consideração os possíveis riscos causados pela coexistência com outros serviços ou subsistemas.

O escopo dos requisitos técnicos e da avaliação se aplicam aos seguintes componentes:

- Componentes do módulo criptográfico:
  - Componentes eletrônicos;
  - *Firmware* e softwares embarcados;
  - Interface de comunicação;
- Mecanismos de segurança física;
- Mecanismos de controle de acesso.

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.

O resultado do processo de homologação informa a aderência aos requisitos técnicos e também atesta aderência a interfaces de interoperabilidade específicas, das quais ao menos uma deve ser suportada:

- Aderência aos requisitos de interoperabilidade ao nível de PKCS#11, informando o ambiente operacional no qual foi analisada a interoperabilidade;
- Aderência aos requisitos de interoperabilidade ao nível de CryptoAPI, informando o ambiente operacional no qual foi analisada a interoperabilidade;
- Aderência aos requisitos de interoperabilidade ao nível de JCE, informando o ambiente operacional no qual foi analisada a interoperabilidade;
- Aderência aos requisitos de interoperabilidade ao nível de OpenSSL, informando o ambiente operacional no qual foi analisada a interoperabilidade;
- Aderência aos requisitos de interoperabilidade ao nível de uma API proprietária, caso utilizada, informando o ambiente operacional no qual foi analisada a interoperabilidade;

1.4 Estruturação do MCT-7

Este documento (MCT-7) está estruturado da seguinte forma:

- Parte 1: Descreve os requisitos técnicos que devem ser verificados no processo de homologação de cartões criptográficos ICP;

- Parte 2: Descreve os materiais que devem ser depositados para a execução do processo de homologação de cartões criptográficos ICP e leitoras de cartões inteligentes;

- Referências normativas: Descreve as referências normativas que foram utilizadas na elaboração deste documento.

2 PARTE 1

Requisitos técnicos para homologação de Módulos de Segurança Criptográficos MSC

2.1 Requisitos Técnicos

A parte 1 deste documento apresenta os requisitos técnicos que devem ser verificados no processo de homologação de módulos de segurança criptográficos.
Os requisitos técnicos descritos nesta parte englobam:

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

Esta seção descreve os requisitos de segurança derivados do padrão americano FIPS 140-2 [FIPS PUB 140-2], publicado pela agência americana NIST. A norma FIPS 140-2 abrange diferentes áreas de atuação relacionadas ao projeto e implementação de um módulo criptográfico. As áreas de atuação contidas no FIPS 140-2 são apresentadas na Tabela 1.

Seção	Áreas de atuação do padrão FIPS 140-2
1	Documentação do módulo criptográfico
2	Identificação de portas e interfaces do módulo criptográfico
3	Nível de identificação de papéis, serviços e autenticação do operador
4	Descrição do modelo de estado finito
5	Nível de segurança física
6	Ambiente operacional
7	Gerenciamento de chaves criptográficas
8	Interferência e compatibilidade eletromagnética
9	Auto-testes
10	Garantia do projeto
11	Mitigação de outros ataques

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

Além das áreas do FIPS 140-2 serão abordados temas neste MCT como:

- Algoritmos criptográficos obrigatórios;
- Gerenciamento;
- Interoperabilidade;

- Restrição de substâncias nocivas.

2.1.1 Requisitos de especificação do módulo criptográfico

DEFINIÇÃO III.1.1: Um módulo criptográfico é um conjunto de hardware, software e *firmware*, ou uma combinação disso que implementa funções criptográficas ou processos, incluindo algoritmos criptográficos e opcionalmente geração de chaves criptográficas. É contido dentro de uma fronteira criptográfica bem definida, portanto é importante saber de cada componente do conjunto e o que passa na fronteira criptográfica como entrada e saída de dados e valores sigilosos.

DEFINIÇÃO III.1.2: A fronteira criptográfica é um perímetro explicitamente definido que estabelece os limites físicos de um módulo criptográfico. Se um módulo criptográfico for composto por componentes de software ou *firmware*, a fronteira criptográfica deve conter o(s) processador(es) e outros dispositivos de hardware que armazenam e protegem os componentes de software e *firmware*. Componentes de hardware, software e *firmware* do módulo criptográfico podem ser excluídos dos requisitos apresentados neste documento, caso tais componentes não afetem a segurança do módulo.

OBSERVAÇÃO: Existem requisitos de documentação descritos a seguir que devem ser atendidos para todos os componentes de hardware, software e *firmware* relacionados à segurança.

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.

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

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.

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.

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

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

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

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 orgão 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.

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.

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.
Esta documentação é obrigatória para o processo de homologação.

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.

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).

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.

RECOMENDAÇÃO III.1.13: O módulo criptográfico também pode suportar a função DSA, conforme o padrão NIST FIPS PUB 186, para autenticação e assinatura digital de dados.

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;
- CCM-MAC baseado nos algoritmos 3DES ou AES, conforme padrão NIST PUB 800-38C).

2.1.2 Portas e interfaces do módulo criptográfico

Um módulo criptográfico possui portas físicas e interfaces lógicas. Segundo o padrão FIPS 140-2, quanto às interfaces lógicas, um módulo pode possuir até quatro tipos de interfaces lógicas:

- Interface de entrada de dados: abrange todos os dados (exceto dados de controle que devem entrar via interface de controle) que devem ser inseridos e processados pelo módulo criptográfico, incluindo, dados em texto claro, dados cifrados, chaves criptográficas, PCS, dados de autenticação e informações de estado de outro módulo;
- Interface de saída de dados: abrange todos os dados (exceto dados ou informações de estado) que devem ser emitidos do módulo criptográfico, incluindo dados em texto claro, dados cifrados, chaves criptográficas, PCS, dados de autenticação e informações de estado de outro módulo. Todos os dados emitidos via "Interface de saída de dados" devem ser inibidos ou impedidos quando um estado de erro ocorrer e durante os auto-testes;
- Interface de entrada de controle: todos os comandos de entrada, sinais e dados de controle (por exemplo, chamadas de funções e controles manuais – comutadores, chaveadores, botões e teclados) usados para controlar a operação do módulo criptográfico devem ser inseridos via "Interface de entrada de controle";
- Interface de saída de estado: todas as informações de estado, indicadores e sinais de saída (por exemplo, códigos de retorno e indicadores físicos – diodos emissores de luz e mostradores/*displays*) usados para indicar o estado do módulo criptográfico devem ser emitidos via "Interface de saída de estado".

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).

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

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.

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.

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.

OBSERVAÇÃO: As portas físicas e interfaces lógicas para a entrada e saída de componentes de chaves criptográficas, dados de autenticação e PCS, devem ser fisicamente e logicamente separadas de qualquer outra porta e interface do módulo criptográfico.
Componentes de chaves criptográficas, dados de autenticação e outras PCS, devem entrar ou sair diretamente do módulo criptográfico (via caminho confiado ou cabo diretamente ligado).

2.1.3 Papéis, serviços e autenticação

Cada operador do módulo criptográfico e o papel que ele pode exigir no módulo precisa ser identificado como forma de controlar o acesso do módulo como os serviços autorizados para cada papel de acesso.
Existem dois tipos de autenticação que podem ser utilizadas em MSCs:

1. Baseado em papel;
2. Baseado em identidade

No primeiro, o operador deve informar um PIN para se autenticar e assumir um dado papel de acesso.

O segundo se refere a uma autenticação onde o papel de acesso é ligado diretamente à identidade do operador, ou seja, somente pela identidade o módulo criptográfico reconhece o papel de acesso relacionado e, portanto, os serviços autorizados para aquela identidade.

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

OBSERVAÇÃO: Um operador não necessita assumir um papel autorizado para realizar um serviço que não divulgue, não modifique, não utilize ou não substitua chaves criptográficas ou PCS ou que não afetem a segurança do módulo. Dentre os serviços que não necessitam de autenticação de operadores estão incluídos:

- Informe de estado;
- Auto-teste.

OBSERVAÇÃO: Múltiplos papéis podem ser assumidos por um mesmo operador.

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.

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.

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

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.

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.

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.

2.1.3.4 Papel de acesso Manutenção

REQUISITO III.3.8: [FIPS 140-2, 4.3.1] 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.

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.

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

2.1.3.5 Serviços

DEFINIÇÃO III.3.1: O termo "serviço" se refere a qualquer serviço, operação ou função que possa ser realizada pelo módulo criptográfico.

DEFINIÇÃO III.3.2: "Entrada de serviço" representa qualquer entrada de dado ou controle que inicie ou realize um serviço, operação ou função específica. "Saída de serviço" representa qualquer saída de dado ou estado resultante de um serviço, operação ou função iniciada por uma "Entrada de serviço". Toda "Entrada de serviço" deve resultar em uma "Saída de serviço".

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.

OBSERVAÇÃO: [observação FIPS 140-2, 4.3.2] Serviços específicos podem ser fornecidos em mais do que um papel de acesso autorizado.

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.

2.1.3.6 Autenticação de operadores do módulo criptográfico

Mecanismos de autenticação podem ser requisitados para autenticar um operador realizando acesso ao módulo criptográfico. Assim, é possível verificar se o operador está autorizado a assumir o papel de acesso requisitado e executar os serviços vinculados a este papel de acesso.
Dependendo do nível de segurança, o módulo criptográfico pode necessitar de diferentes mecanismos de autenticação:

- **Sem autenticação**: Os acessos são realizados sem autenticação;
- **Autenticação baseada em papel de acesso**: O módulo requisita ao operador a seleção de um papel (ou um conjunto de papéis) de acesso e faz a autenticação neste papel. A seleção do papel pode ser explícita ou implícita. O módulo criptográfico não necessita autenticar a identidade individual do operador. Se o módulo criptográfico permitir a um operador alterar seu papel, então o módulo deve autenticar qualquer papel que não foi previamente autenticado;

- **Autenticação baseada em identidades**: O módulo requisita:

  a) que o operador seja individualmente identificado;

  b) que um ou mais papéis sejam, implicitamente ou explicitamente, selecionados pelo operador (seleção de papéis);

  c) autenticar a identidade do operador e a autorização do operador para assumir o papel selecionado.
- A autenticação da identidade do operador, a seleção de papéis e a autorização para assumir os papéis selecionados podem ser combinadas.
- Se o módulo criptográfico permitir a um operador alterar seu papel, então o módulo deve verificar a autorização do operador identificado em assumir qualquer papel que não foi previamente autorizado.

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.

OBSERVAÇÃO: [observação FIPS 140-2, 4.3.3] Um módulo criptográfico pode permitir a um operador autenticado realizar todos os serviços associados ao papel de acesso autorizado, ou pode requisitar uma autenticação separada para cada serviço ou diferentes conjuntos de serviços.

REQUISITO III.3.14: [FIPS 140-2, 4.3.3] Quando o módulo criptográfico for desligado e na seqüência 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.

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.

OBSERVAÇÃO: [observação FIPS 140-2, 4.3.3] A inicialização de mecanismos de autenticação pode necessitar de um tratamento especial. Se o módulo criptográfico não contém os dados de autenticação necessários para autenticar o operador na primeira vez na qual é realizado acesso ao módulo, então outros métodos autorizados (como controles no processo ou dados de autenticação padrão – "*default*") devem ser usados para controlar o acesso ao módulo e iniciar os mecanismos de autenticação.

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.

OBSERVAÇÃO: Para o método de autenticação utilizando PIN como meio, uma probabilidade de 1 em 1.000.000, de que uma tentativa aleatória tenha sucesso, significa PINs de 6 ou mais dígitos.

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.

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.

REQUISITO III.3.19: [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.

2.1.4 Modelo de estado finito

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

REQUISITO 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.

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".

OBSERVAÇÃO: [observação FIPS 140-2, 4.4] Um módulo criptográfico pode, ainda, utilizar outros estados, incluindo, mas não limitado a:

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

REQUISITO 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.

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.

2.1.5 Segurança Física

O módulo criptográfico deve empregar mecanismos de segurança física para restringir acessos não autorizados ao seu conteúdo e também para deter o uso, modificação ou até mesmo substituição não autorizada dos componentes do módulo.

Mecanismos de segurança física de módulos criptográficos são divididos nas seguintes categorias:

- **Proteção que evidencia violação**: São mecanismos de segurança física que envolvem o módulo criptográfico e na tentativa de violação do módulo produzem sinais indicativos e irreversíveis. Estes mecanismos também têm a finalidade de deter a observação, sondagem ou manipulação direta de componentes internos do módulo criptográfico.
- **Proteção que resiste à violação**: São mecanismos de segurança física que envolvem o módulo criptográfico protegendo fisicamente seus principais componentes contra observação, sondagem ou manipulação direta. A tentativa de remover estes mecanismos

de segurança física resulta em danos severos ao módulo criptográfico tornando inutilizável.

- **Proteção que detecta e responde à violação**: São mecanismos de segurança física que envolvem o módulo criptográfico detectando quaisquer tentativas de acesso não autorizado aos seus componentes ou ao seu conteúdo. Na tentativa de observar, sondar ou acessar o módulo criptográfico estes mecanismos destroem quaisquer informações críticas armazenadas em sua memória, como por exemplo, chaves criptográficas ou parâmetros críticos de segurança. A ação destes mecanismos de segurança física não causa a destruição do módulo criptográfico. No entanto, pode ser necessário o envio do módulo ao seu respectivo fabricante para fins de reparos ou reativação.

2.1.5.1 Requisitos gerais de segurança física

Os requisitos técnicos a seguir são aplicáveis a todos os módulos criptográficos, independente dos mecanismos de segurança física implementados.

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.

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.

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.

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.

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.

2.1.5.2 Requisitos específicos para proteção que evidencia violação

Adicionalmente aos requisitos gerais de segurança física, esta seção estabelece os requisitos que devem ser atendidos por todos os módulos criptográficos independente dos mecanismos de segurança física implementados. Os requisitos técnicos desta seção dizem respeito aos mecanismos de segurança física que evidenciam violações.

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.

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.

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.

2.1.5.3 Requisitos específicos de proteção que resiste à violação

Adicionalmente aos requisitos específicos de proteção que evidenciam violações, esta seção estabelece os requisitos que devem ser atendidos por módulos criptográficos, no que diz respeito aos mecanismos de segurança física que resistem à violação.

Esta seção descreve requisitos técnicos aplicáveis à cobertura ou camada que envolve os componentes do módulo criptográfico e/ou o módulo como um todo.

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.

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.

2.1.5.4 Requisitos específicos de proteção que detecta e responde à violação

Adicionalmente aos requisitos específicos de proteção que resiste às violações, esta seção estabelece os requisitos que devem ser atendidos por módulos criptográficos, no que diz respeito aos mecanismos de segurança física que detectam e respondem à violação.

Esta seção descreve requisitos técnicos aplicáveis aos mecanismos de segurança física adicionados à cobertura ou camada que envolve os componentes do módulo criptográfico e/ou o módulo como um todo.

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.

2.1.6 Ambiente operacional

O ambiente operacional de um módulo se refere aos componentes de software, *firmware* e hardware necessários para sua operação.

Um dos principais componentes do ambiente operacional é o sistema operacional (SO). É possível classificar o ambiente operacional de acordo com o tipo de sistema operacional:

[1] **Ambiente operacional não modificável**: Ambiente operacional estático e não modificável;

[2] **Ambiente operacional modificável**: Ambiente operacional passível de ser reconfigurado para adicionar, remover ou modificar funcionalidades. Ambientes operacionais são considerados modificáveis quando os componentes de software ou *firmware* podem ser

modificados por operadores, ou então, quando operadores podem carregar e executar software ou *firmware* que não foi incluído como parte do processo de certificação do módulo.

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.

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.

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.

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.

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".

DEFINIÇÃO III.6.1: Caminho confiável (*Trusted path*): um caminho protegido entre o operador e o MSC com o qual ambos acreditam que estejam interagindo. Um caminho confiável

reflete um canal protegido. O software malicioso que se injeta neste caminho pode ser identificado.
Um caminho confiável pode ser visto como um mecanismo que fornece autenticidade entre o operador e o módulo criptográfico, garantindo que ataques não consigam interceptar ou modificar informações sendo transmitidas no caminho.

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.

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.

2.1.7 Gerenciamento de chaves criptográficas

O gerenciamento de chaves criptográficas abrange o ciclo de vida completo das chaves criptográficas, seus componentes e PCSs empregados pelo módulo. Abrange a geração de números aleatórios, a geração de chaves, a atribuição de chaves (conforme definido no item 3.7.4), a entrada e saída de chaves, o armazenamento de chaves e a sobrescrita do valor da chave com zeros.

DEFINIÇÃO III.7.1: Chave criptográfica cifrada se refere a uma chave que é cifrada utilizando um algoritmo de segurança aprovado pela família de padrões do grupo do Comitê Gestor da ICP-Brasil.

DEFINIÇÃO III.7.2: PCS cifrado se refere a um PCS que é cifrado utilizando um algoritmo de segurança aprovado pela família de padrões do grupo do Comitê Gestor da ICP-Brasil.

OBSERVAÇÃO: Chaves criptográficas e PCSs cifrados utilizando um algoritmo de segurança não aprovado pela família de padrões do grupo do Comitê Gestor da ICP-Brasil, serão considerados em formato de texto claro.

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.

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

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

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.

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.

2.1.8 Geradores de números aleatórios

O módulo pode empregar geradores de números aleatórios (*Random Number Generators* - RNG) determinísticos ou não determinísticos aprovados pela família de padrões FIPS para a geração de chaves criptográficas.

O termo "geradores de números aleatórios determinísticos aprovados" compreendem os algoritmos referenciados no FIPS 140-2 Anexo C

- FIPS 186-2 – apêndice 3.1 e 3.2
- ANSI X9.31 – apêndice A.2.4 com AES ou 3DES de 3 chaves
- ANSI X9.62 – Anexo A.4

Estes métodos são conhecidos como geradores de pseudo-aleatoriedade e podem ser referenciados como métodos PRNG.

O termo "geradores de números aleatórios não determinísticos" compreendem métodos de geração de números aleatórios por hardware ou, por exemplo, via coleta de entropia de um sistema operacional (movimento de mouse, teclado, lentidão de rede, etc).

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).

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).

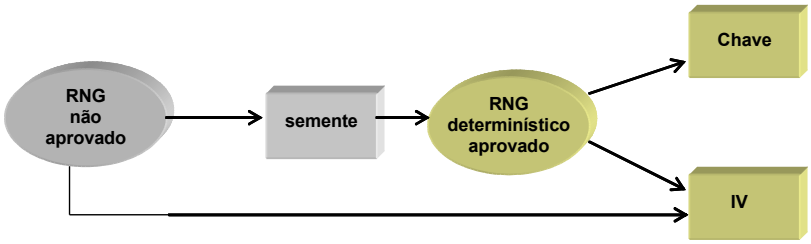

Figura 1. Geradores de números aleatórios

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.

2.1.9 Geração de chaves criptográficas

Um módulo criptográfico pode gerar chaves criptográficas internamente.

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.

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.

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”).

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).

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.

2.1.9.2 Importação e exportação de chaves criptográficas

Chaves criptográficas podem ser importadas (inseridas) ou exportadas (retiradas) de um módulo criptográfico usando um método manual (via teclado, por exemplo) ou um método eletrônico (por exemplo: utilizando uma mídia de armazenamento, *token* de memória, cartão criptográfico, *token* criptográfico, etc).

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.

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.

OBSERVAÇÃO: [observação FIPS 140-2, 4.7.4] Uma chave pública pode ser importada ou exportada do módulo criptográfico em texto claro.

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.

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).

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

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*).

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.

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.

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.

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.

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

2.1.9.4 Atribuição de chaves

DEFINIÇÃO III.7.3: O processo de atribuição de chaves (*key establishment*) possibilita atribuir uma chave simétrica para uso criptográfico aos participantes legítimos de uma sessão de comunicação. A atribuição de chaves pode ser realizada por um processo automático (protocolo de negociação de chaves ou protocolo de transporte de chaves), método manual ou uma combinação dos anteriores.

DEFINIÇÃO III.7.4: Um método manual de atribuição de chaves é aquele no qual é utilizado um dispositivo de armazenamento para o transporte manual da chave.

DEFINIÇÃO III.7.5: Um protocolo de negociação de chaves (*key agreement*) possibilita atribuir uma chave simétrica aos participantes legítimos em função de valores secretos definidos por cada um dos participantes, de forma que nenhum dos participantes possa pré-determinar o valor da chave. Neste método, a chave não é transferida, nem mesmo de forma cifrada. Exemplo desta classe de protocolo é o algoritmo *Diffie-Hellman*.

DEFINIÇÃO III.7.6: Um protocolo de transporte de chaves (*key transport*) possibilita que uma chave simétrica seja transferida aos participantes legítimos da entidade geradora para os parceiros. Neste método, a chave é definida por uma das entidades e repassada às demais.

REQUISITO III.7.24: [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.

REQUISITO III.7.25: [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).

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.

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.

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).

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

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.

OBSERVAÇÃO: [observação FIPS 140-2, 4.7.6] A sobrescrita com zeros binários do valor de chaves criptográficas ou PCSs que estejam cifrados não é obrigatória.

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.

2.1.10 Interferência/compatibilidade eletromagnética

A definição formal dada à "Compatibilidade Eletromagnética" (EMC – *Electromagnetic Compatibility*) pelo Vocabulário Internacional de Eletrotécnica (IEC50) é a "capacidade de um dispositivo, equipamento ou sistema funcionar satisfatoriamente no seu ambiente eletromagnético sem introduzir nenhuma perturbação eletromagnética intolerável ao ambiente, ou seja, não produzir adversamente uma perturbação eletromagnética que prejudique o funcionamento de outros equipamentos, e também, não ser afetado pelos outros equipamentos neste mesmo ambiente". O objetivo da EMC é minimizar a influência de ruídos dessa espécie.
A Interferência Eletromagnética (EMI – *Electromagnetic Interference*) pode ser vista como um tipo de poluição que degrada o ambiente à volta do equipamento emissor e que pode ser comparável à poluição sonora, química ou qualquer outra que descarrega algo indesejável no ambiente. A EMI pode ser responsável pelo mal funcionamento ou degradação do desempenho de outros equipamentos.

Os testes de EMI/EMC são necessários para se assegurar o funcionamento correto do equipamento em seu ambiente, mantendo um grau aceitável de 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).

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

2.1.11 Auto-testes

Um módulo criptográfico deve realizar auto-testes na hora de ligar o módulo para assegurar que está funcionando corretamente. Se um auto-teste falhar, o módulo criptográfico estará comprometido e não pode ser mais considerado confiável.

REQUISITO III.9.1: [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.

REQUISITO III.9.2: [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".

REQUISITO III.9.3: [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.

REQUISITO III.9.4: [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.

REQUISITO III.9.5: [FIPS 140-2, 4.9] A documentação do módulo criptográfico deve especificar os seguintes itens:

- Os autotestes 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).

2.1.11.1 Testes de energização

Testes realizados quando o módulo criptográfico é energizado:

- Testes de algoritmos criptográficos;
- Testes de números aleatórios;

- Testes da integridade de software/firmware;
- Testes de funções criticas;
- Outros testes realizados na energização ou sob demanda.

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)

REQUISITO III.9.7: [FIPS 140-2, 4.9.1] Os testes de energização serão executados automaticamente 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).

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

2.1.11.2 Testes condicionais

Testes realizados quando as seguintes condições do teste ocorrer:

- Testes de consistência de pares (se o módulo criptográfico gera chaves públicas e privadas);
- Testes de carregamento de Software/*Firmware*;
- Testes de entrada manual de chaves;
- Teste do gerador de números aleatórios do tipo "contínuo" (*continuous test*) para o gerador de números aleatórios por hardware;
- Outros testes condicionais.

Se o módulo criptográfico gerar chaves públicas e privadas os testes de consistência em pares de chaves públicas e privadas devem ser realizados.

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.

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.

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.

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.

OBSERVAÇÃO: [FIPS 140-2, 4.9.2] As chaves criptográficas ou componentes de chaves devem ter um código de detecção de erro aplicado, ou devem ser colocados utilizando entradas duplicadas.

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.

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.

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.

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 seqüência deve ser comparado com o bloco previamente gerado. O teste deve falhar se qualquer dos dois blocos de n bits 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.

2.1.12 Garantia de projeto

Garantia de projeto se refere ao uso de melhores práticas pelo fabricante do módulo criptográfico durante o processo de elaboração do projeto, distribuição e operação de um módulo criptográfico, fornecendo garantia que o módulo criptográfico é testado devidamente, configurado, entregue, instalado, desenvolvido e possui garantia de fornecimento de documentação apropriada para os operadores.
Requisitos de segurança são especificados para gerenciamento de configuração e operação além de documentos de usuário.

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.

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

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.

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.

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.

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.

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.

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.

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.

2.1.13 Mitigações de ataques

Esta seção apresenta requisitos técnicos que dizem respeito aos ataques ao módulo criptográfico classificados como ataques invasivos. Estes ataques podem ser aplicados em módulos criptográficos que se encontram em ambientes hostis, com por exemplo, ambientes onde o próprio operador do módulo é o atacante. Alguns tipos de ataques abordados dependem da análise de informações que são obtidas externamente ao módulo e que permitem determinar algum conhecimento a respeito das chaves criptográficas e PCSs contidas no módulo criptográfico.

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.

REQUISITO III.11.2: A documentação técnica do módulo criptográfico deve especificar quais outros tipos de ataques são mitigados pelo módulo.

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).

2.2 Requisitos de gerenciamento

Os requisitos de gerenciamento se referem a funcionalidades que devem estar disponíveis aos operadores do módulo criptográfico, permitindo executar operações de controle.
Por exemplo:

- Gerenciamento de meios de autenticação
- *Backup* e recuperação de chaves
- Importação de chaves

- Visualização de chaves
- Logs de acesso e operações realizadas

2.2.1 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;

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;

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.

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

DEFINIÇÃO IV.1.1: Seja "N" um número pré-definido de pessoas (operadores) que possuem acesso ao sistema do MSC. "N" deve ser um número inteiro maior ou igual a 1.

DEFINIÇÃO IV.1.2: Seja "M" um subconjunto de "N" de pessoas (operadores) que possuem acesso ao sistema do MSC. "M" deve ser um número inteiro menor ou igual a "N".

DEFINICÃO IV.1.3: Sistema de segredo compartilhado "M de N" é um método de segurança para as chaves criptográficas do MSC. No mínimo "M" pessoas das "N" cadastradas devem estar presentes para o acesso às operações do sistema de MSC.
Esse método previne ações unilaterais dos operadores do MSC através da divisão da senha de acesso ao MSC em "N" partes. A chave só será reconstruída se no mínimo "M" partes de "N" proverem a sua senha (parte) individual.
Um exemplo comumente usado nesse caso é o de "3 de 5", onde a senha de acesso ao MSC é dividida em 5 partes e no mínimo, necessitará de 3 dessas 5 pessoas para acessar o MSC.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

2.3.1.2 Requisitos sobre CryptoAPI

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

REQUISITO V.1.5: O módulo criptográfico deve suportar, no mínimo, uma implementação do MS CryptoAPI, versão 1.0.

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*.

- **REQUISITO V.1.7:** A implementação de MS CryptoAPI deve suportar os algoritmos criptográficos descritos na seção 3.1.1, "Algoritmos Criptográficos Obrigatórios".

2.3.1.3 Requisitos sobre PKCS#11

OBSERVAÇÃO: Requisitos sobre PKCS#11 devem ser avaliados apenas se esta API for implementada.

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

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.

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

2.3.1.4 Requisitos sobre Java Cryptographic Extension (JCE)

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

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

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*

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

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

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.

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.

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

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.

2.3.1.5 Requisitos sobre OpenSSL

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

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.*

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

2.3.2 Requisitos de armazenamento

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

REQUISITO V.2.2: Deve ser possível por meio de um dos APIs listados na seção 4.1 chamar funções que retornam a capacidade de armazenamento do módulo criptográfico.

2.4 Requisitos para restrição de substâncias nocivas

A RoHS (*Restriction to the use of Hazardous Substances*) é uma diretiva da União Européia (2002/95/EC) que estabelece a restrição ao uso de certas substâncias consideradas nocivas na fabricação de certos tipos de produtos/equipamentos eletroeletrônicos.
Esta diretiva entrou em vigor a partir de 1° de julho de 2006 e todos os produtos/equipamentos que não estiverem em conformidade não poderão ser comercializados na Europa e nem em outros países que estejam seguindo a diretiva estabelecida, a menos que estejam dentro de uma lista de exceções já estabelecida.

A WEEE (*Waste from Electrical and Electronic Equipment*) lida com o tratamento, recuperação e reciclagem de resíduos de materiais eletroeletrônico dispensados.
Em alguns países fora do continente europeu há regras e normas compatíveis, semelhantes ou derivadas da RoHS e WEEE que também visam à preservação da saúde humana e do meio-ambiente em relação às substâncias nocivas pelo contato ou exposição prolongada.
As substâncias abordadas e consideradas banidas pela diretiva RoHS são:

- Metais pesados:
  - Chumbo (Pb)
  - Mercúrio (Hg)
  - Cromo Hexavalente ou Cromo VI (Cr(VI))

- Cádmio (Cd)

- Retardantes de chamas:
  - Bromobifenilas (PBB)
  - Éteres de Bromobifenilas (PBDE)

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.

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.

Observação: Entende-se como material homogêneo uma substância simples, como por exemplo, plástico do encapsulamento de componentes, ou ainda, a solda dos contatos em um circuito integrado. Um componente eletrônico como um transistor ou capacitor não são materiais, mas contém diversos materiais homogêneos.

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.

2.5 Requisitos de documentação

Para o processo de homologação é fundamental possuir a documentação correta para avaliar questões que não envolvem o hardware do MSC diretamente.

Existem dois tipos de documentação que devem ser consideradas para o processo de homologação de MSC:

1. Documentação do produto;
2. Documentação técnica.

A documentação técnica será detalhada ao longo do texto nas seções específicas onde constam os requisitos de documentação essencialmente técnica necessária para o entendimento e caracterização de determinada funcionalidade ou operação do MSC.

A documentação será aceita nas línguas: português do Brasil e inglês.

A documentação do produto em geral envolve os seguintes itens:

- **Manual de instalação**: Manual especificando como será feita a instalação física do MSC caso ele seja do tipo que depende de uma máquina como um servidor para funcionar (placa PCI, PCMCIA, etc).
- **Manual de configuração**: Manual especificando os recurso de configuração do MSC.
- **Manual do operador**: Manual do usuário, especificando tarefas como gerenciamento de chaves que não precisam da autenticação do administrador.
- **Manual do administrador (SO)**: Manual do administrador (*Security Officer)* que gerencia a configuração do MSC, tais como criar os usuários e slots (*tokens*) de acesso ao MSC.
- **Manual do desenvolvedor**: Manual da API proprietária do MSC para desenvolver aplicações utilizando o MSC. Especificação do próprio fornecedor.
- **Manual de integração**: Manual de APIs de mercado como PKCS#11, CryptoAPI, SUN JCE, dentre outras.

- **Manual de importação de chaves**: Manual especificando a utilização de outros hardwares específicos como *smart cards*, leitoras de *smart cards* ou *tokens* criptográficos utilizados para carregar chaves criptográficas no MSC.

O MCT de materiais a serem depositados (MCT-11) terá um *check-list* com uma lista completa de documentação requisitada para o processo de homologação de MSCs, subdividida em seções referenciadas neste documento.

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.

REQUISITO VII.2: A PI deve fornecer o manual de instalação, especificando os sistemas operacionais suportados pelo MSC.

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.

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

OBSERVAÇÃO: Os administradores (SO) também devem possuir acesso a estes recursos.

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

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.

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.

3 PARTE 2

Material e documentos técnicos a serem depositados para a execução do processo de homologação de Módulos de Segurança Criptográficos

3.1 Depósito de materiais e documentos técnicos

Esta parte detalha os materiais e os documentos técnicos a serem depositados pela parte interessada junto ao LSI-TEC/LEA para a execução dos processos de homologação de Módulos de Segurança Criptográficos (MSCs) no âmbito da ICP-Brasil.

Os materiais e os documentos técnicos são classificados em três categorias:

1. Componentes físicos: correspondem às amostras de MSCs a serem submetidas ao processo de homologação, bem como leitoras de cartões inteligentes, cartões e *tokens* criptográficos para apoio no processo de controle de acesso ao módulo criptográfico;
2. Documentos técnicos: correspondem aos documentos de natureza técnica referentes aos dispositivos a serem submetidos ao processo de homologação. Devem ser depositados em formato impresso ou em formato eletrônico. No caso de formato eletrônico, devem estar armazenados, preferencialmente, em mídia tipo "leitura-somente" (*read-only*). Devem estar, obrigatoriamente, escritos nas línguas portuguesa ou inglesa;
3. Componentes em softwares executáveis: correspondem aos CSPs, drivers, bibliotecas de software, ferramentas de gerenciamento de dispositivo e/ou outros softwares executáveis, solicitados por este documento, referentes aos dispositivos a serem submetidos ao processo de homologação. Devem ser depositados obrigatoriamente em formato eletrônico e armazenados preferencialmente em mídia tipo "leitura-somente" (*read-only*).

Três Níveis de Segurança da Homologação (NSH) foram estabelecidos para a homologação de MSCs:

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

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

1. Linguagem de alto nível: Código-fonte deve ser depositado, por exemplo, em linguagem C, C++ ou Java. Se o código-fonte estiver escrito em linguagem proprietária ou mesmo em microcódigo, o respectivo manual desta linguagem deve estar contido na documentação bem como compiladores e simuladores para compilação e execução deste código-fonte;
2. Linguagem de baixo nível: Código-fonte deve ser depositado em linguagem *assembly*, porém acompanhado do respectivo manual das instruções desta linguagem bem como compiladores e simuladores para compilação e execução desse código-fonte;

Adicionalmente aos Níveis de Segurança de Homologação, são estabelecidos dois Níveis de Segurança Física (NSF):

- NSF 1: Este nível requer que o módulo criptográfico suporte no mínimo os mecanismos de segurança física que evidenciam e resistem à violação. A análise de conformidade contemplará os requisitos das seções 2.1.5.1, 2.1.5.2 e 2.1.5.3.
- NSF 2: Além dos mecanismos de segurança física que são suportados no NSF 1, este nível requer que o módulo criptográfico suporte também mecanismos de segurança física que detectam e respondem à violação. A análise de conformidade contemplará os requisitos das seções 2.1.5.1, 2.1.5.2, 2.1.5.3 e 2.1.5.4.

A parte interessada deve especificar qual o Nível de Segurança Física desejado para homologação.

3.2 Material e documentos técnicos a serem depositados

3.2.1 Componentes físicos

Independemente do NSH e NSF escolhido pela parte interessada, os seguintes componentes físicos devem ser depositados junto ao LSI-TEC/LEA:

- Módulo de segurança criptográfico operacional: Amostras de MSC operacionais nas quantidades definidas por este documento para cada modelo e/ou versão de MSC a ser submetido ao processo de homologação.
- Módulo de segurança criptográfico não operacional: Amostras de MSC não operacionais, com características idênticas, nas quantidades definidas por este documento para cada modelo e/ou versão de MSC a ser submetido ao processo de homologação.

- Componentes de segurança física: Amostras de cada componente responsável por garantir um determinado tipo de segurança física no módulo criptográfico, como por exemplo, micro switches, sensores ou outros dispositivos conforme o Nível de Segurança Física pretendido.
- Material de apoio: Caso o MSC submetido necessite de hardware de apoio como cartão inteligente, leitora ou *token*, serão necessárias quantidades mínimas para operação do módulo criptográfico.

3.2.2 Documentos técnicos

3.2.3 Nível de Homologação 1

3.2.4 Manuais do produto

Os seguintes documentos técnicos devem ser depositados junto ao LSI-TEC/LEA pela parte interessada:

Manual – Nível de segurança da homologação 1, 2, 3
Instalação
Configuração
Operadores
Administrador (Security Officer)
Desenvolvedor
Integração
Importação de chaves

3.2.5 Documentação técnica específica

Os seguintes documentos técnicos específicos devem ser depositados junto ao LSI-TEC/LEA pela parte interessada:

MCT-7 Seção 3.1 – Especificação do módulo criptográfico

Documentação – Nível de segurança da homologação 1, 2, 3	check
Componentes de hardware, software e firmware	
Fronteira criptográfica	
Configuração física do módulo	
Componentes de hardware, software ou firmware que estejam excluídos dos requisitos de segurança	
Especificação de todas as portas físicas, interfaces lógicas e caminhos de dados (entrada/saída)	
Controles lógicos e manuais	
Indicadores de estados lógicos e físicos	
Características elétricas, lógicas e físicas	
Especificação das funções de segurança e operações criptográficas empregadas pelo módulo	
Diagrama de blocos detalhando todos os principais componentes de hardware e de interconexão	
Projeto de design dos componentes de hardware, software e firmware	
Dados relacionados à segurança e onde são armazenados nos componentes de hardware	
Política de segurança adotada pelo módulo criptográfico.	

MCT-7 Seção 3.2 – Portas e Interfaces

Documentação – Nível de segurança da homologação 1, 2, 3	check
Interfaces lógicas presentes	
Interface de entrada de dados	
Interface de saída de dados	
Entrada de controle	
Saída de estado	

MCT-7 Seção 3.3 – Papéis, serviços e autenticação

Documentação – Nível de segurança da homologação 1, 2, 3	check
Controle de acesso empregado pelo módulo	
Mecanismo de autenticação (baseado em papel ou identidade)	
Os tipos de dados de autenticação	
Especificar os papéis autorizados suportados	
Funcionalidades atribuídas ao papel de acesso “Usuário”	
Funcionalidades atribuídas ao papel de acesso “Oficial de Segurança”	
Funcionalidades atribuídas ao papel de acesso “Manutenção”	
Serviços empregados pelo módulo	
Entradas e saídas de serviços	
Papéis de acesso autorizados nos quais o serviço pode ser realizado	
Serviços fornecidos sem autenticação	
Especificar a força ou robustez dos mecanismos de autenticação	

MCT-7 Seção 3.4 – Modelo de estado finito

Documentação – Nível de segurança da homologação 1, 2, 3	check
Diagrama de transição de estados e/ou a tabela de transição de estados	
Estados operacionais e estados de erro	
Estados de desvio (bypass)	
Estados de manutenção	
Representação do modelo de estado finito (ou equivalente)	

MCT-7 Seção 3.5 – Segurança física

Documentação	check
Descrição de todos os componentes de hardware, software, firmware que estão contidos na fronteira criptográfica e protegidos pelos mecanismos de segurança física implementados.	
Descrição dos mecanismos de segurança física implementados no módulo criptográfico e seus respectivos componentes	
Descrição de portas, tampas ou interfaces de acesso para manutenção	
Descrição dos mecanismos de destruição de chaves criptográficas simétricas e assimétricas privadas e PCSs	

Documentação	check
Descrição dos sensores para portas, tampas ou interfaces presentes no módulo	

MCT-7 Seção 3.6 – Ambiente operacional

Documentação – Nível de segurança da homologação 1, 2, 3	check
Especificar o ambiente operacional utilizado	
Especificar o sistema operacional (SO) utilizado (caso propósito geral)	
Documentação de homologações existentes do SO	
Documentação de homologações existentes do ambiente operacional	
Especificar o conjunto de papéis que podem ativar a execução do software e firmware	
Especificar o conjunto de papéis que podem modificar componentes de software ou firmware	
Especificar o conjunto de papéis que podem ler componentes armazenados no módulo	
Especificar o conjunto de papéis que podem inserir chaves criptográficas e PCS.	
Especificar acesso por meio de outros processos nas chaves privadas e secretas em texto claro, CSPs e valores intermediários de geração de chaves	
Especificar a funcionalidade de SO de mecanismos de auditoria para registrar modificações, acessos, apagamentos e adições nos dados criptográficos e PCS	
Especificar a utilização de caminho confiável (Trusted path)	

MCT-7 Seção 3.7 – Gerenciamento de chaves criptográficas

Documentos – Nível de segurança da homologação 1, 2, 3	check
Especificar todas as chaves criptográficas, seus componentes e PCS empregados pelo módulo.	
Especificar quais métodos são utilizados pelo módulo criptográfico para proteger chaves secretas, chaves privadas e PCS contra divulgação, modificação e substituição não autorizada.	
Especificar quais métodos são utilizados pelo módulo criptográfico para proteger chaves públicas contra modificação e substituição não autorizada.	
Especificar cada método de RNG empregado pelo módulo, seja ele aprovado ou não pelo padrão FIPS.	
Especificar cada um dos métodos de geração de chaves criptográficas empregados pelo módulo (aprovados ou não pela família de padrões FIPS).	
Especificar os métodos de atribuição de chaves (conforme definido no item 3.7.4) empregados pelo módulo criptográfico (automático, manual ou combinação dos anteriores).	
Especificar os métodos de importação e exportação de chaves criptográficas empregados pelo módulo (métodos aprovados ou não pela família de padrões FIPS).	
Especificar os métodos de armazenamento de chaves criptográficas empregados pelo módulo.	
Especificar os métodos de sobrescrita de chaves criptográficas com zeros binários que são empregados pelo módulo.	

MCT-7 Seção 3.8 – Interferência/Compatibilidade eletromagnética

Documentos	check
Documentos comprovando conformidade do equipamento às normas de EMI/EMC para equipamentos de tecnologia da informação compatíveis com as normas reconhecidas internacionalmente.	
Documentos constando o nome do laboratório responsável onde foi obtida para o equipamento a certificação de conformidade EMI/EMC para equipamentos de tecnologia da informação.	
Documentos devem citar a qual órgão regulador o laboratório está credenciado.	

MCT-7 SEÇÃO 3.9 – AUTO-TESTES

Documentos – Nível de segurança da homologação 1, 2, 3	check
Especificar os auto-testes realizados pelo módulo criptográfico	
Estados de erro em que o módulo criptográfico pode entrar	
Condições e ações necessárias para sair dos estados de erro e reiniciar a operação	
Testes de funções criptográficas do tipo "resposta conhecida" chamadas na etapa de auto-teste	
Testes de consistência de pares	
Testes de carregamento de Software/Firmware	
Testes de entrada manual de chaves	
Teste do gerador de números aleatórios do tipo "contínuo"	
Especificar o código de detecção de erro aplicado para teste de integridade de firmware	

MCT-7 SEÇÃO 3.10 – GARANTIA DE PROJETO

Documentos – Nível de segurança da homologação 1	check
Manuais dos operadores	
Documentos – Nível de segurança da homologação 2	
Código-fonte de firmware e outros componentes externos	

MCT-7 SEÇÃO 3.11 – MITIGAÇÕES DE ATAQUES

Documentos	check
Proteção contra ataques não invasivos	
Proteção contra outros tipos de ataques	

MCT-7 SEÇÃO 4 – GERENCIAMENTO DO MSC

Documentos	check
Atualização de firmware	
Sistema de back-up de chaves	
Especificação da ativação M de N	
Utilitários de administração e diagnósticos	

MXT-7 SEÇÃO 5 – INTEROPERABILIDADE

Documentos	check
Especificação da capacidade de armazenamento	

MCT-7 SEÇÃO 6 – RESTRIÇÃO DE SUBSTÂNCIAS NOCIVAS

Documentos	check
Equipamento deve estar em conformidade com as regras da Diretiva da União Européia (2002/95/EC) de Restrição às Substâncias Nocivas (RoHS)	
Documentação deve detalhar 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	
Certificado dos fornecedores de materiais, peças, componentes ou partes integrantes do equipamento final atestando a conformidade com a diretiva da RoHS	

3.2.5.1 Documentação geral

Os seguintes documentos técnicos devem ser depositados junto ao LSI-TEC/LEA pela parte interessada:

- Política de segurança não proprietária: Política de segurança não proprietária (pública) de acordo com o programa de validação de módulos criptográficos mantido pelo NIST, especificamente quanto ao padrão FIPS 140-2;
- Relação de certificados obtidos: Relação de certificações e/ou licenças obtidas de entidades independentes para o módulo criptográfico;
- Outros documentos: Projetos técnicos e suas especificações que a parte interessada julgar necessários para completar toda documentação técnica exigida.

3.2.6 Nível de Segurança da Homologação 2

Adicionalmente à documentação técnica solicitada no NSH 1 (seção 3.2.3), os seguintes itens devem ser depositados junto ao LSI-TEC/LEA pela Parte Interessada:

- Código-fonte do componente PRNG *(Pseudo Random Number Generator);*
- Código-fonte do componente de geração de chaves;
- Código-fonte do componente de sobrescrita de chaves;
- Código-fonte do componente de atribuição de chaves (conforme definido no item 3.7.4);
- Código-fonte do componente de armazenamento de chaves;

- Código-fonte do componente de importação/exportação de chaves e sementes;

3.2.7 Nível de Segurança da Homologação 3

Adicionalmente à documentação técnica solicitada no NSH 1 (seção 3.2.3) e NSH 2 (seção 3.2.6), os seguintes itens devem ser depositados junto ao LSI-TEC/LEA pela parte interessada:

- Código-fonte embarcado: Relação de todo código-fonte de software e/ou *firmware* embarcados no MSC;
- Código-fonte de apoio: Relação de todo código-fonte de apoio relacionado às interfaces de programação (API), SDK (*Software Development Kits*), SP (*Service Providers*), CSP, ferramenta de gerenciamento e bibliotecas de software suportadas pelo módulo criptográfico.

3.3 Componentes em software executável

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

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

4 Quantidades de materiais e documentos técnicos a serem depositados

Esta seção apresenta os materiais e os documentos técnicos a serem depositados pela parte interessada junto ao LSI-TEC/LEA referente ao processo de homologação de MSCs.

As quantidades de material e documentos técnicos apresentados nesta seção devem seguir os seguintes critérios:

- Quanto aos componentes físicos: devem ser entregues ao LSI-TEC/LEA 1 (uma) amostra operacional e 2 (duas) amostras não operacionais para cada modelo e/ou versão de MSC a ser submetido ao processo de homologação;
    - Componentes de segurança física: devem ser entregues ao LSI-TEC/LEA 3 (três) amostras operacionais de cada tipo de componente utilizado na segurança física do módulo criptográfico
    - Material de apoio: no contexto do MSC entregue deve incluir o seguinte material
        - Leitora de cartão inteligente: amostras necessárias para a utilização de mecanismos de controle de acesso implementados por meio de cartão inteligente;
        - Cartão inteligente: amostras necessárias para utilização de mecanismos de controle de acesso implementados por meio de cartão inteligente;
        - *Token* criptográfico: amostras necessárias para utilização de mecanismos de controle de acesso implementados por meio de *token* criptográfico;
- Quanto à documentação técnica:
    - Documentos impressos (Documentos técnicos): cópias de igual teor (por exemplo, três cópias impressas do manual de segurança do módulo criptográfico);
    - Documentos eletrônicos (Documentos técnicos): cópias de igual teor e armazenadas, obrigatoriamente, em mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como documentos técnicos o manual de usuário, a política de segurança não proprietária, o manual da ferramenta de gerenciamento e código-fonte);
- Quanto aos componentes em softwares executáveis: cópias de igual teor e armazenadas, obrigatoriamente, em mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como componentes em softwares executáveis, a ferramenta de gerenciamento do módulo criptográfico e o CSP do módulo criptográfico).

- Tabela 2. Quantidade de materiais e documentos técnicos a serem depositados

Requisito de depósito	Materiais e documentos técnicos a serem depositados pela parte interessada – NSH 1	quant
1	MSC (Módulo de segurança criptográfico)	1
2	MSC não operacional	2
3	Componentes de segurança física (para cada tipo)	3
4	Cartão inteligente	-
5	Leitora de cartão inteligente	-
6	Token de acesso	-
7	PIN padrão para os cartões inteligentes ou tokens	-
8	Documentação específica	2
9	Política de segurança não proprietária	2
10	Manual de usuário e manual de instalação	2
11	Manuais das interfaces de programação (APIs) e bibliotecas de desenvolvimento	2
12	Manual da ferramenta de gerenciamento do cartão inteligente	2
13	Manual(is) de provedor(es) de serviço	2
14	Relação de certificados obtidos	2
15	Outros documentos	2
Requisito de depósito	**Materiais e documentos técnicos a serem depositados pela parte interessada – NSH 2**	
16	Código-fonte do componente PRNG (Pseudo Random Number Generator);	2
17	Código-fonte do componente de geração de chaves;	2
18	Código-fonte do componente de atribuição de chaves (conforme definido no item 3.7.4);	2
19	Código-fonte do componente de sobrescrita de chaves;	2
20	Código-fonte do componente de armazenamento de chaves;	2
21	Código-fonte do componente de importação/exportação de chaves e sementes;	2
Requisito de depósito	**Materiais e documentos técnicos a serem depositados pela parte interessada – NSH 3**	
22	Código-fonte embarcado	2

Requisito de depósito	Materiais e documentos técnicos a serem depositados pela parte interessada – NSH 1	quant
23	Código-fonte de apoio	2
Requisito de depósito	**Componentes em software executável a serem depositados pela parte interessada – NSH 1, 2 e 3**	
24	Provedor(es) de serviço criptográfico	2
25	Ferramenta de gerenciamento do módulo criptográfico	2
26	Outras bibliotecas de software e/ou programas	2

Requisito de depósito
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Requisito de depósito
16
17
18
19
20
21
Requisito de depósito

Requisito de depósito
22
23
Requisito de depósito
24
25
26

5 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 Infraestrutura 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 Infraestrutura de Chaves Públicas Brasileira (ICP-BRASIL).** Brasília. ICP-BRASIL: 2006.

[14] [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.

[15] [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.

[16] [FCC] **CODE OF FEDERAL REGULATIONS 47 PART 15 - RADIO FREQUENCY DEVICES - SUBPART B - UNINTENTIONAL RADIATORS**. 2007.

[17] [IEC. CISPR 22] **LIMITS AND METHODS OF MEASUREMENT OF RADIO DISTURBANCE CHARACTERISTICS OF ITE**. 2006.

[18] [IEC. CISPR 24] **LIMITS AND METHODS OF MEASUREMENT OF THE IMMUNITY CHARACTERISTICS OF ITE**. 1997.

[19] [IEC 60050 - 161] **INTERNATIONAL ELECTROTECHNICAL VOCABULARY**. 1990.

[20] 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) – ISO/IEC 8825-1.** Genève, Switzerland, Reference Number: ISO/IEC 8825-1:2002.

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

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

[23] [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.

[24] [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>

[25] [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.

[26] [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.

[27] [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.

[28] [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.

[29] [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.

[30] [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.

[31] [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.

[32] [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.

[33] [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.

[34] [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.

[35] [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.

[36] [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.

[37] [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.

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

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

[40] [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.

[41] [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.nov.2006.

[42] [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.nov.2006.

[43] [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.

[44] [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.

[45] [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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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 III.5.6	3

REQUISITO	Quantidade de ensaios
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 III.7.30	5

REQUISITO	Quantidade de ensaios
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