LEA

Requisitos Técnicos para Homologação de Módulos de Segurança Criptográficos no âmbito da ICP-Brasil

versão 1.0 preliminar 20

São Paulo, 18 de junho de 2007.

Título	Requisitos Técnicos para Homologação de Módulos de Segurança Criptográficos no âmbito da ICP-Brasil
Versão	versão 1.0 preliminar 20
Data	18 de junho de 2007
Autor(es)	Mads Rasmussen, Edson Alonso, Marcelo Bortolotto, Artur Gasparetto Paiola, Igor Medeiros, Gerson Faria, Adilson Guelfi
Classificação	Público

Sumário

Listas de Ilustrações

Lista de Figuras

Lista de Tabelas

Controle de Versão

Versão revisada	Data de emissão	Alterações realizadas

Glossário

Assinatura Digital	Resultado de uma transformação criptográfica de dados, que quando implementada apropriadamente, provê os seguintes serviços de segurança: autenticação, integridade de dados e não-repudiação do signatário.
Chave Criptográfica	Código ou parâmetro usado em conjunto com um algoritmo criptográfico, determinando as seguintes operações: • Transformação de dados em texto claro para um formato cifrado e vice-versa; • Assinatura digital computada a partir de dados; • Verificação de uma assinatura digital computada a partir de dados; • Geração de um código de autenticação computado a partir de dados; ou • Um acordo para troca de um segredo compartilhado.
Chave Secreta	Ver “Chave simétrica”
Chave Pública	Chave criptográfica, usada com um algoritmo criptográfico de chave pública, distribuída livremente para todos os correspondentes via e-mail ou outras formas.
Chave Privada	Chave criptográfica, usada com um algoritmo criptográfico de chave pública, a qual deve ser conhecida apenas pelo seu proprietário.
Chave simétrica	Chave criptográfica, usada com um algoritmo criptográfico de chave simétrica, que está unicamente associada a uma ou mais entidades e não deve tornar-se pública.

Módulo Criptográfico	Um módulo criptográfico é composto por componentes de hardware, software e *firmware* que implementam funções ou processos criptográficos contidos dentro de uma fronteira criptográfica.
Operador	Um indivíduo ou processo que realiza operações no módulo criptográfico.
Integridade	Propriedade que determina que dados não devem ser modificados ou apagados de uma maneira não autorizada e indetectável
Interface	Representa um ponto lógico de entrada e saída de dados, que provê acesso aos serviços disponíveis pelos softwares.
Software	Programas e componentes de dados usualmente armazenados em mídias que podem ser apagadas (disco rígido, por exemplo), os quais podem ser dinamicamente escritos e modificados durante a execução.
Interface Própria	Interface de programação própria fornecida pelo fabricante como meio de interagir com o HSM
Hardware Security Module (HSM)	É um dispositivo baseado em hardware que gera, guarda e protege chaves criptográficas, além de ter a capacidade de executar operações criptográficas, como assinatura digital.

Lista de Acrônimos

AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
API	Application Program Interface
CBC	Cipher Block Chaining
CMAC	Cypher-based Message Authentication Code
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
HMAC	Keyed-hash Message Authentication Code
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICP	Infra-Estrutura de Chaves Públicas
ICP-Brasil	Infra-Estrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OID	Object Identifier
PCS	Parâmetros Críticos de Segurança
PIN	Personal Identification Number – uma senha alfanumérica
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PP	Protection Profile
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
SDK	Software Developement Kit
SHA	Secure Hash Algorithm

TI	Tecnologia de Informação
URL	Uniform Resource Locator

1 Introdução

Este documento descreve os requisitos técnicos a serem observados no processo de homologação de Hardware Security Modules (HSMs) no âmbito da Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil

Para uma melhor compreensão do disposto neste documento, entenda-se por:

- Hardware Security Module: um servidor de segurança fisicamente seguro, resistente à violação que fornece funcionalidades criptográficas com capacidade de geração e armazenamento de chaves criptográficas simétricas e assimétricas voltados para utilização em uma Infra-estrutura de Chaves Públicas (ICP).

Neste documento, o termo "módulo criptográfico" será usado em referência ao processador criptográfico interno do HSM.

1.1 Objetivo da homologação

O objetivo do processo de homologação de HSMs é propiciar a interoperabilidade e operação segura do serviço criptográfico ICP oferecido 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 HSM para garantia da interoperabilidade e operação segura.

Os requisitos técnicos englobam requisitos de documentação, requisitos de segurança, requisitos de gerenciamento e requisitos de interoperabilidade que devem ser atendidos pelo HSM.

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 de depósito de material.

A figura 1 apresenta uma visão geral do processo de homologação.

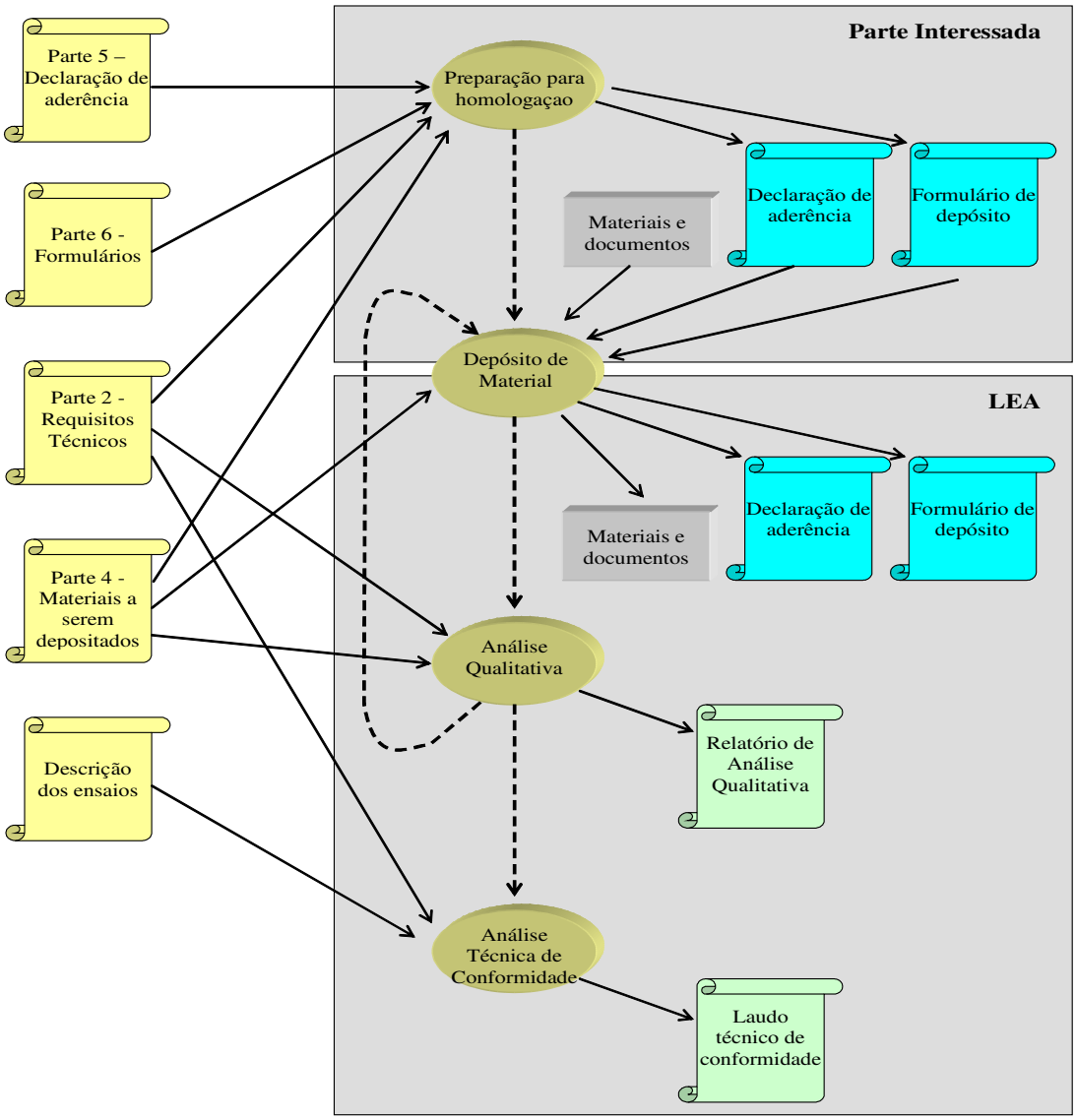

Figura 1: Processo de Homologação

1.3 Documentos relacionados

O manual de condutas técnicas volume (MCT-10) é composto por 6 partes:

- Parte 1 – Visão geral e vocabulário;
- Parte 2 – Requisitos técnicos;
- Parte 3 – Descrição dos ensaios;
- Parte 4 - Materiais a serem depositados;
- Parte 5 – Declaração de aderência;
- Parte 6 – Formulários;

1.4 Escopo do processo de homologação

Um HSM pode oferecer suporte a outros serviços ou subsistemas, coexistindo de forma integrada ou não com o serviço criptográfico 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 serviço criptográfico ICP, porém levando em consideração os possíveis riscos causados pela coexistência com outros serviços ou subsistemas.

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

- Componentes do módulo criptográfico:
  - Componentes eletrônicos;
  - Firmware e softwares embarcados;
  - Interface de comunicação;
- Nível de segurança física
- Nível de controle de acesso
- Módulo de softwares de provedores de serviço;

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

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

2 Requisitos de Documentação

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

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

1. Documentação do produto
2. Documentação técnica

A documentação técnica será especificada ao longo do texto nas seções específicas onde aparecem os requisitos de documentação altamente técnica para entender ou especificar algum funcionamento específico do HSM.

A documentação do produto em geral envolve os seguintes itens:

- **Manual de instalação**: Manual especificando como será feita a instalação física do HSM 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 HSM.
- **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 HSM, tais como criar os usuários e slots (*tokens*) de acesso ao HSM.
- **Manual do desenvolvedor**: Manual da API nativa do HSM para desenvolver aplicações utilizando o HSM. 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 smartcards, leitoras de smartcards ou tokens criptográficos utilizados para carregar chaves criptográficas no HSM.

O MCT de materiais de depósito (MCT-11) terá um check-list com uma lista completa de documentação requisitada para o processo de homologação de HSMs.

REQUISITO II.1: A PI deve fornecer manual de instalação, especificando a arquitetura de máquina em qual é suportado a instalação do HSM.

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

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

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

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

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

REQUISITO II.6: A PI deve fornecer o manual de desenvolvedor detalhando a API nativa para desenvolvimento de aplicações (SDK) utilizando o HSM.

REQUISITO II.7: A PI deve fornecer o manual de integração do HSM com as API´s de mercado para desenvolvimento de sistemas integrados.

REQUISITO II.8: A PI deve fornecer manual de importação de chaves detalhando a aplicabilidade do uso de outros hardwares com o HSM.

3 Requisitos de segurança FIPS 140-2

Esta seção descreve os requisitos segurança derivados ao padrão FIPS 140-2, o padrão FIPS 140-2 [FIPS PUB 140-2] publicado pelo NIST abrange diferentes áreas de atuação relacionadas ao projeto e implementação de um módulo criptográfico. As áreas de atuação contidas no padrão 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 nesse MCT como

- Algoritmos criptográficos obrigatórios
- Gerenciamento
- Interoperabilidade
- Restrição de substâncias nocivas

3.1 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: [FIPS 140-2, 4.1] 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: [FIPS 140-2, 4.1] A parte interessada deve fornecer documentação específica que descreve a configuração física do módulo.

REQUISITO III.1.3: [FIPS 140-2, 4.1] A parte interessada deve fornecer documentação especifica 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: [FIPS 140-2, 4.1] 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.

REQUISITO III.1.5: [FIPS 140-2, 4.1] A parte interessada deve fornecer documentação específica dos controles lógicos e manuais do módulo.

REQUISITO III.1.6: [FIPS 140-2, 4.1] A parte interessada deve fornecer documentação específica dos indicadores de estados lógicos e físicos do módulo.

REQUISITO III.1.7: [FIPS 140-2, 4.1] A parte interessada deve fornecer documentação específica das características elétricas, lógicas e físicas aplicáveis ao módulo.

REQUISITO III.1.8: [FIPS 140-2, 4.1] 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. Essa documentação pode ser um manual do operador ou até uma política de segurança do FIPS 140-2 se o objeto de homologação previamente foi submetido para homologação no NIST.

REQUISITO III.1.9: [FIPS 140-2, 4.1] A parte interessada deve fornecer documentação cotendo 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 listado em cima.

REQUISITO III.1.10: [FIPS 140-2, 4.1] 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 do FIPS 140-2 se o objeto de homologação previamente foi submetido para homologação no NIST.

REQUISITO III.1.11: [FIPS 140-2, 4.1] 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 pode comprometer a segurança do módulo criptográfico.

REQUISITO III.1.12: [FIPS 140-2, 4.1] 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).

3.2 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.2.1: O módulo criptográfico deve suportar no mínimo as seguintes funções criptográficas:

- Criptografia de Dados:
  - DES (*Data Encryption Standard*) no modo de operação ECB e CBC, apenas para uso legado (conforme padrão NIST FIPS PUB 46-3);

- *Triple*-DES (3DES ou TDES) no modo de operação ECB e CBC (conforme padrão NIST FIPS PUB 46-3);
- AES (*Advanced Encryption Standard*) com tamanho de chave 128 bits no modo 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 1024 bits (conforme padrões ANSI X9.31 e PKCS#1 v. 1.5).
- Resumo Criptográfico de Dados (*Hash*):
  - SHA-1 (conforme padrão NIST FIPS PUB 180-2, Secure Hash Algorithm)
  - SHA-256 (conforme padrão NIST FIPS PUB 180-2, Secure Hash Algorithm)

RECOMENDAÇÃO III.2.1:: De forma opcional, sugere-se que o módulo criptográfico também possa suportar a função AES (*Advanced Encryption Standard*) com tamanho de chaves maiores de 192 e 256 bits (conforme padrão NIST FIPS PUB 197) para criptografia de dados.

RECOMENDAÇÃO III.2.2: Devido os avanços tecnológicos em fatoração de números compostos , sugere-se de forma opcional, que o módulo criptográfico também possa suportar a função RSA com tamanho de chaves maior de 1024 bits (ex. 1536 ou 2048 bits) para autenticação e assinatura de dados.

RECOMENDAÇÃO III.2.3: De forma opcional, sugere-se que o módulo criptográfico também possa suportar a função DSA (*Data Signature Algorithm*) com tamanho de chaves maior de 512 bits (conforme padrão NIST FIPS PUB 186) para autenticação e assinatura de dados.

RECOMENDAÇÃO III.2.4: De forma opcional, sugere-se que o módulo criptográfico também possa suportar as seguintes funções para a geração de resumos criptográficos de dados (conforme padrão NIST FIPS PUB 180-2, Secure Hash Algorithm):

- SHA-224;
- SHA-384;
- SHA-512.

RECOMENDAÇÃO III.2.5: De forma opcional, sugere-se que o módulo criptográfico também possa suportar as seguintes funções para a autenticação de dados

- CBC-MAC baseado no 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 no 3DES ou AES (conforme padrão NIST PUB 800-38B)
- MAC algoritmo CCM baseado no 3DES ou AES (Counter with Cipher Block Chaining-Message Authentication Code conforme padrão NIST PUB 800-38C)

3.3 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 deve 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"; e
- 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.3.1: [FIPS 140-2] Energia elétrica externa (incluído energia de uma fonte de energia externa ou baterias) que entra no módulo Criptográfico deve utilizar uma porta de energia. Uma porta de energia não é necessária quando toda energia é fornecida ou mantida internamente pelo módulo criptográfico (por ex. Uma bateria interna)

REQUISITO III.3.2: [FIPS 140-2] Devem ser informadas todas as interfaces lógicas presentes no módulo criptográfico.

REQUISITO III.3.3: [FIPS 140-2] O módulo criptográfico deve assegurar que o fluxo de informação e acesso físico sejam realizados pelas portas físicas e interfaces lógicas relacionadas.

REQUISITO III.3.4: [FIPS 140-2] 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.3.5: [FIPS 140-2] 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: [observação FIPS 140-2 para níveis 1 e 2] As portas físicas e interfaces lógicas para a entrada e saída de componentes de chaves criptográficas, dados de autenticação e PCS podem ser compartilhadas fisicamente e logicamente com outras portas e interfaces do módulo criptográfico.

OBSERVAÇÃO: [observação FIPS 140-2 no nível 3] 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 ser inseridas diretamente no módulo criptográfico (via caminho confiado ou cabo diretamente ligado)

3.4 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 HSMs:

1. Baseado em papel; e
2. Baseado em identidade

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

O segundo refere-se a uma autenticação onde a 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.4.1: 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 incluem-se:

- Informe de estado;
- Auto-teste;

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

REQUISITO III.4.2: [FIPS 140-2, 4.3] O módulo criptográfico pode 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.

3.4.1 Papéis de Acesso

REQUISITO III.4.3: [FIPS 140-2, 4.3.1] O módulo criptográfico deve suportar, no mínimo, os seguintes "papéis autorizados":

- **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 (*key zeroization*), etc;
- **Oficial de segurança (SO)**: Necessário para realizar funções de gerenciamento, inicialização, distribuição e fechamento de acesso ao módulo.

Se o módulo criptográfico permite operadores realizar serviços de manutenção física e/ou serviços de manutenção lógica, deve suportar o seguinte papel autorizado:

- **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 armazenada em texto claro assim como CSPs não protegidos devem ser "zerados" quando da entrada ou saída do papel de manutenção.

OBSERVAÇÃO: Caso não exista o papel de manutenção, o oficial de segurança deve realizar as funções de manutenção e auditoria.

REQUISITO III.4.4: [FIPS 140-2, 4.3.1] A documentação deve especificar todos os papéis autorizados que são suportados pelo módulo criptográfico.

REQUISITO III.4.5: Funcionalidades atribuídas ao papel de acesso "Usuário" devem incluir:

- Manipulação (leitura, escrita, criação e remoção) de elementos no sistema de arquivos do 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;
- Sobrescrita do valor de chaves criptográficas com zeros “0” (*key zeroization*);
- Finalização do módulo criptográfico;
- Execução de auto-testes;
- Requisição de informações de estado do módulo criptográfico.

3.4.1.1 Papel de “Oficial de Segurança” (SO)

REQUISITO III.4.6: Durante a inicialização do módulo criptográfico, o papel “Oficial de Segurança” deve ser autenticado, informando seu PIN correspondente, ou seja, o PIN do Oficial de Segurança ou identidade por meio de token ou chave física.

REQUISITO III.4.7: Funcionalidades atribuídas ao papel de acesso “Oficial de Segurança” devem incluir:

- Inicialização do sistema de arquivos do módulo criptográfico;
- Geração de chaves RSA;
- Distribuição do módulo criptográfico;
- 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.

3.4.1.2 Papel de Manutenção

REQUISITO III.4.8: [FIPS 140-2, 4.3.1] Se o módulo criptográfico permite aos operadores realizar serviços de manutenção, o módulo deve suportar o seguinte papel de acesso autorizado:

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

OBSERVAÇÃO: Caso o HSM não suporte um papel específico de manutenção, as operações de manutenção será feita pelo oficial de segurança (SO).

REQUISITO III.4.9: [FIPS 140-2, 4.3.3] Se o módulo criptográfico permite aos operadores realizar serviços de manutenção, o módulo deve suportar o seguinte papel de acesso autorizado:

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

REQUISITO III.4.10: [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.4.11: 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

3.4.2 Serviços

DEFINIÇÃO III.4.1: O termo "serviço" refere-se a qualquer serviço, operação ou função que possa ser realizada pelo módulo criptográfico.

DEFINIÇÃO III.4.2: “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.4.12: [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 aprovada. 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.4.13: [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 no qual o serviço pode ser realizado; e
- 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.

3.4.3 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); e

  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.4.14: [FIPS 140-2 nível 2, 4.3.3] O módulo criptográfico deve empregar o mecanismo de autenticação baseada 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.4.15: [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.4.16: [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

contem 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.4.17: [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.

REQUISITO III.4.18: [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.4.19: [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.4.20: [FIPS 140-2, 4.3.3] Caso o módulo utilize dispositivos de hardware no processo de autenticação, a documentação do módulo criptográfico deve especificar:

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

3.5 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.5.1: [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; e

d) Os eventos de saída resultantes das transições de um estado para outro.

REQUISITO III.5.2: [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 diferenciar-se 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; e 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] O módulo criptográfico pode, ainda, utilizar outros estados, incluindo, mas não limitado a:

- Estados de desvio (bypass): Estados em quais capacidade de desvio está ativada e serviços estão oferecidos sem processamentos criptográfico.
- Estados de manutenção: Estados para manutenção e prestação de serviços ao módulo criptográfico, incluindo testes de manutenção lógicos e físicos. Se o módulo criptográfico contem um papel de acesso de manutenção, então um estado de manutenção deve ser incluído.

OBSERVAÇÃO: Não está aceito qualquer tipo de desvio na homologação de equipamentos HSM no âmbito ICP-Brasil.

REQUISITO III.5.3: [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, incluído inserções de dados e controles, que causam transições de um estado para outro; e

– Os eventos de saída, incluído condições internas do módulo criptográfico, saídas de dados, e saídas de estado resultantes de transições de um estado para outro.

3.6 Segurança Física

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

Os requisitos que dizem respeito a segurança física de módulos criptográficos são divididos em três categorias de acordo com o nível de segurança física oferecido pelo mecanismos de proteção empregados no módulo.

- **Proteção simples**: São mecanismos de segurança física que já estão presentes nos componentes do módulo criptográfico desde o processo de fabricação de cada componente. Em muitos casos, tais mecanismos de segurança possuem apenas a função principal de dar rigidez ao componente, e como conseqüência fornecem também proteção física ao módulo. A tentativa de remover este mecanismo de proteção pode acarretar em mal funcionamento do módulo.
- **Proteção que evidencia violação**: São mecanismos de segurança física que são adicionados aos componentes do módulo criptográfico, após o processo de fabricação. Na presença de tentativa de violação do módulo criptográfico, este tipo de mecanismo de segurança produz sinais indicativos irreversíveis de que houve tentativa de violar o módulo. A tentativa de remover este mecanismo de proteção pode também destruir fisicamente o módulo, tornando-o inutilizável.
- **Proteção que detecta violação**: São mecanismos de proteção que podem ser adicionados ou podem envolver externamente todo o módulo criptográfico. Quando existe a tentativa de observação do conteúdo do módulo, de maneira não autorizada, estes mecanismos entram em ação para destruir a informação contida no módulo. A

tentativa de burlar tal mecanismo de segurança pode resultar, além da perda de informações, também na inoperância do módulo sendo necessário o envio do mesmo para fins de reparos junto ao seu respectivo fabricante.

3.6.1 Requisitos gerais de segurança física

Os requisitos técnicos a seguir são aplicáveis a todos os tipos de mecanismos de segurança física de módulos criptográficos.

REQUISITO III.6.1: A documentação técnica do módulo criptográfico deve especificar todos os componentes de hardware, software, firmware que estão contidos na fronteira criptográfica e protegidos pelos mecanismos de segurança física implementados.

REQUISITO III.6.2: A documentação técnica do módulo criptográfico deve especificar quais mecanismos de segurança física estão implementados no módulo e seus respectivos componentes, conforme as categorias de mecanismos de segurança física descritas no início da Seção 2.6.

REQUISITO III.6.3: Se o módulo criptográfico incluir interface de acesso para manutenção que requer acesso físico ao conteúdo do módulo criptográfico, como por exemplo, pelo fabricante do módulo criptográfico ou qualquer outro indivíduo autorizado, então:

- A interface de acesso para manutenção deve ser composta por todos os caminhos de acesso físico ao conteúdo do módulo criptográfico, incluindo quaisquer coberturas removíveis ou portas;
- Quaisquer coberturas removíveis ou portas inclusas dentro da interface de acesso para manutenção devem ser protegidas utilizando mecanismos apropriados de segurança;

- Todas as chaves criptográficas simétricas e assimétricas privadas em texto claro e PCSs devem ser apagadas quando a interface de acesso para manutenção for utilizada;

REQUISITO III.6.4: A documentação técnica do módulo criptográfico deve descrever, se aplicável, 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.6.5: Se o módulo criptográfico possuir portas ou coberturas removíveis, então o módulo deverá possuir sensores que detectam o acesso a estas portas ou interfaces.

REQUISITO III.6.6: Quando ocorrer o acesso físico a portas, tampas ou interfaces de acesso para manutenção, os sensores que detectam o acesso a estas portas devem iniciar instantaneamente no módulo criptográfico um processo de destruição de chaves secretas, chaves em texto claro ou PCSs desprotegidos e que estão armazenados em seu interior.

REQUISITO III.6.7: Se o módulo criptográfico possuir orifícios ou fendas para ventilação, então estes devem ser construídos de forma a prevenir qualquer tipo de sondagem ou observação indevida do interior do módulo.

3.6.2 Requisitos específicos para proteção simples

REQUISITO III.6.8: O módulo criptográfico deve consistir de componentes que incluem mecanismos de segurança física simples, como por exemplo, cobertura aplicada sobre os componentes do módulo criptográfico, durante o processo de fabricação, para proteção contra danos físicos ou ambientais.

REQUISITO III.6.9: A cobertura/camada que protege fisicamente os componentes do módulo criptográfico deve ser opaca ao espectro de luz visível.

3.6.3 Requisitos específicos para proteção que evidencia violação

REQUISITO III.6.10: Os componentes do módulo criptográfico devem ser revestidos por uma cobertura/camada que evidencie violações de tentativa de acesso físico ao módulo com o intuito de deter a observação, sondagem ou manipulação direta do módulo, portanto, provendo evidências de tentativa de violar ou remover componentes do módulo.

REQUISITO III.6.11: A cobertura/camada que evidencia violações dos componentes do módulo criptográfico deve ser opaca ao espectro de luz visível.

REQUISITO III.6.12: A cobertura/camada que reveste os componentes do módulo criptográfico deve consistir de um material rígido que evidencia violações, como por exemplo, material a base de resina epoxy. A tentativa de remoção deste material deve oferecer alto risco de causar danos severos ao módulo criptográfico, podendo resultar em não funcionamento do módulo.

3.6.4 Requisitos específicos de proteção que detecta violação

REQUISITO III.6.13: Os componentes do módulo criptográfico devem estar contidos em um invólucro ou cobertura removível, que deve ser composto de um material plástico rígido ou material metálico.

REQUISITO III.6.14: O invólucro que envolve todos os componentes do módulo criptográfico deve ser opaco ao espectro de luz visível.

REQUISITO III.6.15: Os componentes do módulo criptográfico devem ser revestidos por uma cobertura/camada resistente a corrosão.

REQUISITO III.6.16: A cobertura/camada resistente a corrosão que reveste os componentes do módulo criptográfico deve ser opaca ao espectro de luz visível.

REQUISITO III.6.17: O módulo criptográfico deve estar todo contido em um invólucro plástico rígido ou metálico, e que pode também possuir portas ou coberturas removíveis.

REQUISITO III.6.18: Quando o invólucro que envolve o módulo criptográfico possuir portas ou coberturas removíveis, estas deverão ser fechadas com cadeados resistentes a violações que empregam chaves físicas ou lógicas, ou protegidas por lacres que evidenciam violações.

REQUISITO III.6.19: O revestimento que envolve os circuitos do módulo criptográfico deve ser coberto com um material rígido plástico ou material metálico (como por exemplo, a base de resina epoxy), o qual deve ser opaco no espectro de luz visível.

3.6.5 Requisitos específicos para módulos criptográficos do tipo multi-chip "standalone"

REQUISITO III.6.20: O módulo criptográfico deve estar totalmente contido em um invólucro de plástico rígido ou metálico que pode possuir portas ou coberturas removíveis.

REQUISITO III.6.21: O invólucro que envolve todo o módulo criptográfico deve ser opaco ao espectro de luz visível.

REQUISITO III.6.22: Quando o invólucros que envolve o módulo criptográfico possuir portas ou coberturas removíveis, estas deverão ser fechadas com cadeados resistentes a violações que empregam chaves físicas ou lógicas protegidas por lacres que evidenciam violações.

REQUISITO III.6.23: O revestimento que envolve os circuitos do módulo criptográfico deve ser coberto com um material rígido (como por exemplo, a base de resina epoxy), o qual é opaco no espectro de luz visível.

REQUISITO III.6.24: O módulo criptográfico deve estar contido em um invólucro resistente, tal que, qualquer tentativa de remoção ou penetração deste invólucro oferece um alto risco de causar danos severos ao módulo criptográfico, ou seja, o módulo não funcionará.

3.7 Ambiente Operacional

O ambiente operacional de um módulo refere-se 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 de propósito geral:** Refere-se ao uso de um sistema operacional de propósito geral e comercial.

[2] **Ambiente operacional limitado**: Ambiente operacional estático e não modificável, não baseado num sistema operacional de propósito geral para seu suporte;

[3] **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.7.1: [FIPS 140-2, 4.6] A documentação deve especificar o ambiente operacional utilizado pelo módulo criptográfico, incluindo, se aplicável, o sistema operacional (SO) utilizado pelo módulo criptográfico.

3.7.1 Ambiente operacional de propósito geral

REQUISITO III.7.2: [FIPS 140-2, 4.6] A documentação deve especificar o sistema operacional (SO) utilizado pelo módulo criptográfico.

REQUISITO III.7.3: [FIPS 140-2, 4.6] No caso em que o sistema operacional (SO) utilizado pelo módulo criptográfico já foi homologado em relação ao 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.

3.7.2 Ambiente operacional limitado

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

REQUISITO III.7.4: [FIPS 140-2, 4.6] No caso em que o ambiente operacional utilizado pelo módulo criptográfico já foi homologado em relação ao alguma norma nacional ou internacional como FIPS 140-2 da NIST, Common Criteria da ISO/IEC ou outra, a PI deve fornecer documentação dessa homologação.

3.7.3 Ambiente operacional modificável

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

REQUISITO III.7.5: [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 discreto (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.7.6: [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, CSPs e valores intermediários de geração de chaves enquanto o módulo estiver executando e operacional.

REQUISITO III.7.8: [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”; e
- 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”; e
- Associação e retirada de uma função para o papel de “Oficial de Segurança”.

DEFINIÇÃO III.7.1: Caminho confiável (*Trusted path*): um caminho protegido entre o operador e o HSM com o qual ambos acreditam que estejam interagindo. Um caminho confiável reflete um canal protegido. O software malicioso que injeta-se neste caminho pode ser identificado.

Um caminho confiável pode ser visto como um mecanismo que fornece confidencialidade de que o operador realmente está comunicando com o que ele está tentando comunicar, garantindo que ataques não consigam interceptar ou modificar informações sendo transmitida no caminho.

REQUISITO III.7.9: [FIPS 140-2 nível 2, 4.6] Todas as chaves criptográficas e PCS, dados de autenticação, entradas de controle e saídas de status devem comunicar através de um mecanismo confiável que utiliza portas físicas de I/O dedicadas ou caminho confiável.

RECOMENDAÇÃO III.7.1: [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; e
- Identificação do origem e do destino de um caminho confiável.

3.8 Gerenciamento de Chaves Criptográficas

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

DEFINIÇÃO III.8.1: Chave criptográfica cifrada refere-se a uma chave que é cifrada utilizando um algoritmo de segurança aprovado pela família de padrões FIPS.

DEFINIÇÃO III.8.2: PCS cifrado refere-se a um PCS que é cifrado utilizando um algoritmo de segurança aprovado pela família de padrões FIPS.

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

REQUISITO III.8.1: [FIPS 140-2, 4.7] Chaves secretas, chaves privadas e PCS devem estar protegidas dentro do módulo contra divulgação, modificação e substituição não autorizada.

REQUISITO III.8.2: [FIPS 140-2, 4.7] Chaves públicas devem estar protegidas dentro do módulo contra modificação e substituição não autorizada.

REQUISITO III.8.3: [FIPS 140-2, 4.7] A documentação deve especificar todas as chaves criptográficas, seus componentes e PCS empregados pelo módulo.

REQUISITO III.8.4: [requisito complementar ao FIPS 140-2] A documentação deve especificar quais métodos são usados pelo módulo criptográfico para proteger chaves secretas, chaves privadas e PCS contra divulgação, modificação e substituição não autorizada.

REQUISITO III.8.5: [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.

3.8.1 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.

Pelo termo "geradores de números aleatórios determinísticos aprovados" entende-se 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.

Pelo termo "geradores de números aleatórios não determinísticos" entende-se 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.8.6: [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 (ver Figura 2).

REQUISITO III.8.7: [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 (ver Figura 2).

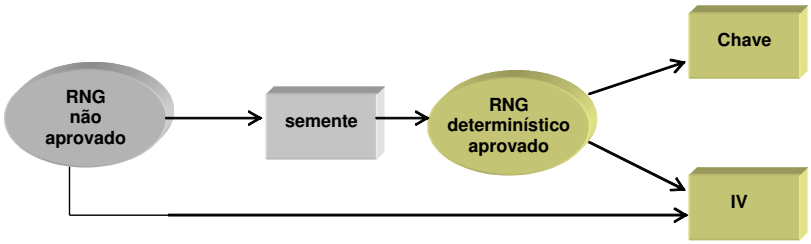

Figura 2. Geradores de Números Aleatórios

REQUISITO III.8.8: [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.

3.8.2 Geração de Chaves Criptográficas

Um módulo criptográfico pode gerar chaves criptográficas internamente.

REQUISITO III.8.9: [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.8.10: [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.8.11: [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 3.8.4(“Importação e Exportação de Chaves Criptográficas”).

REQUISITO III.8.12: [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).

3.8.2.1 Requisitos específicos de Geração de Chaves Criptográficas

REQUISITO III.8.13: Quando geradas internamente ao módulo criptográfico, chaves criptográficas devem ser, obrigatoriamente, configuradas com um dos seguintes atributos: exportável ou não exportável.

3.8.3 Atribuição de Chaves

DEFINIÇÃO III.8.3: 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.8.4: 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.8.5: 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.8.6: 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.8.14: [FIPS 140-2, 4.7.3] Se métodos de atribuição de chaves são empregados pelo módulo criptográfico, então somente os métodos de atribuição de chaves aprovados pela família de padrões FIPS devem ser usados.

REQUISITO III.8.15: [FIPS 140-2, 4.7.3] Quando aplicável, a documentação deve especificar os métodos de atribuição de chaves empregados pelo módulo criptográfico (automático, manual ou combinação dos anteriores).

3.8.4 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.8.16: [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.8.17: [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 níveis 1 e 2, 4.7.4] Uma chave criptográfica simétrica ou assimétrica privada quando importada ou exportada do módulo criptográfico utilizando um método manual pode ser manipulada em texto claro.

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

REQUISITO III.8.18: [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.8.19: [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.8.20: [FIPS 140-2, 4.7.4] Chaves importadas manualmente deve ser verificadas durante a entrada no módulo criptográfico utilizando o teste especificado na seção 3.10.2

REQUISITO III.8.21: [FIPS 140-2, 4.7.4, níveis de segurança 2 e 3] Chaves secretas e privadas importadas utilizando métodos automáticos devem entrar no módulo criptográfica cifradas.

REQUISITO III.8.22: [FIPS 140-2, 4.7.4, níveis de segurança 2 e 3] Chaves secretas e privadas importadas utilizando métodos manuais devem entrar no módulo criptográfica ou sair do módulo criptográfico ou

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

REQUISITO III.8.23: [FIPS 140-2, 4.7.4, níveis de segurança 2 e 3] Caso o compartilhamento de conhecimento (split knowledge) está 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 inserido ou extraído 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.
- Documentação deve provar tecnicamente que, se conhecimento de *n* componentes de chaves está necessários para recompor a chave, o conhecimento de *n-1* componentes não fornece nenhuma informação sobre a chave original além do tamanho da chave

3.8.4.1 Requisitos Específicos de Exportação de Chaves Criptográficas

REQUISITO III.8.24: 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.8.25: Deve ser possível configurar no módulo criptográfico com atributo não exportável, uma chave criptográfica simétrica e/ou assimétrica privada, 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.8.26: Chaves assimétricas públicas podem ser exportadas do módulo criptográfico.

3.8.5 Armazenamento de Chaves Criptográficas

REQUISITO III.8.27: [FIPS 140-2, 4.7.5] Chaves criptográficas devem ser armazenadas dentro do módulo criptográfico em texto claro ou de forma cifrada.

REQUISITO III.8.28: [FIPS 140-2, 4.7.5] Chaves privadas e secretas em texto claro não devem ser acessíveis por operadores não autorizados.

REQUISITO III.8.29: [FIPS 140-2, 4.7.5] O módulo criptográfico deve associar à cada chave (simétrica ou assimétrica) armazenada a seu respectiva operador (pessoa, grupo, processo, servidor, etc.).

REQUISITO III.8.30: [FIPS 140-2, 4.7.5] A documentação deve especificar os métodos de armazenamento de chaves criptográficas empregados pelo módulo.

3.8.5.1 Sobrescrita do Valor de Chaves Criptográficas com Zeros Binários

REQUISITO III.8.31: [FIPS 140-2, 4.7.6] O módulo deve prover métodos para sobrescrever com zeros binários os valores de todas as chaves simétricas, chaves assimétricas privadas e PCS.

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

REQUISITO III.8.32: [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.

3.9 Interferência/Compatibilidade Eletromagnética

A definição formal dada a 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.9.1: [requisito FIPS 140-2, item 4.8] A parte interessada deve 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.9.2: [requisito FIPS 140-2, item 4.8] A parte interessada deve 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 a qual órgão regulador o laboratório está credenciado.

3.10 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.10.1: [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 3.10.1 e 3.10.2.

REQUISITO III.10.2: [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.10.3: [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.10.4: [FIPS 140-2, 4.9] Quando um estado de erro ocorrer devido a falhas em um auto-teste, toda saída ou envio de dados via "Interface de Saída de Dados" deve ser impedido.

REQUISITO III.10.5: [FIPS 140-2, 4.9] A documentação do módulo criptográfico deve especificar os seguintes itens:

- Os auto-testes realizados pelo módulo;
- Os estados 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).

3.10.1 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.10.6: [FIPS 140-2, 4.9.1] Os testes de energização será executados pelo módulo criptográfico quando o módulo é energizado (depois de ser desligado, reinicializado, reinicialização do SO, etc.)

REQUISITO III.10.7: [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 (encriptação, decriptação, autenticação e geração de números aleatórios)

REQUISITO III.10.8: [FIPS 140-2, 4.9.1] A documentação deve listar todos os testes de funções criptográficos do tipo "resposta conhecida".

3.10.2 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"

- Outros testes condicionais

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

REQUISITO III.10.9: [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 podem ser carregados externamente para dentro do módulo criptográfico, o seguinte teste de carregamento de software/firmware será executado.

REQUISITO III.10.10: [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.10.11: [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.

Se chaves criptográficas ou componentes de chaves são colocados para dentro do módulo manualmente, o seguinte teste de entrada manual de chaves criptográficos deve ser realizado.

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.10.12: [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.10.13: [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.10.14: [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 seguinte teste do gerador de números aleatórios.

REQUISITO III.10.15: [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.10.16: [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 será utilizado, mas armazenado para comparação com os próximos n bits gerados. Cada subseqüência de n bits gerado deve ser

comparado com os n bits previamente gerado. O teste deve falhar se qualquer das seqüências comparadas de n bits forem iguais.

3.11 Garantia de Projeto

Garantia de projeto refere-se 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 segurança que o módulo criptográfico é testado devidamente, configurado, entregue, instalado, desenvolvido e possui garantia de fornecimento de documentação apropriado para os operadores.

Requisitos de segurança são especificados para gerenciamento de configuração e operação além de documentos de usuário.

REQUISITO III.11.1: [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.11.2: [FIPS 140-2, 4.10] A documentação deve listar procedimentos específicos de instalação segura e inicialização do módulo criptográfico.

REQUISITO III.11.3: [FIPS 140-2, 4.10] A documentação deve especificar a relação entre o projeto dos componentes do hardware, software e firmware do módulo criptográfico.

Nível de Segurança 1

REQUISITO III.11.4: [FIPS 140-2, 4.10] O documentação "Guia do Administrador" (*Crypto Officer*) deve especificar:

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

REQUISITO III.11.5: [FIPS 140-2, 4.10] O documentação "Guia do Usuário" deve especificar:

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

Nível de Segurança 2

REQUISITO III.11.6: [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.11.7: [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 linguagem de baixo nível.

REQUISITO III.11.8: [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.11.9: [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) é tido como essencial em relação ao desempenho ou quando a linguagem de alto nível não estiver disponível.

Nível de Segurança 3

REQUISITO III.11.10: [FIPS 140-2, 4.10] A documentação deve especificar um modelo formal que descreva as regras e características da política de segurança do módulo criptográfico. O modelo formal pode ser especificado usando uma linguagem de especificação formal, tais como modelos baseados em notações matemáticas.

REQUISITO III.11.11: [FIPS 140-2, 4.10] A documentação deve especificar uma justificativa que demonstre a consistência e completude do modelo formal com a respectiva política de segurança do módulo criptográfico.

REQUISITO III.11.12: [FIPS 140-2, 4.10] A documentação deve especificar uma prova informal da correspondência do modelo formal e a especificação funcional.

REQUISITO III.11.13: [FIPS 140-2, 4.10] Para cada componente do módulo criptográfico de hardware, software e firmware, o código-fonte deve conter comentários que descrevam as pré-condições requeridas na entrada no componente, função do procedimento do módulo criptográfico, de modo a executá-lo corretamente e as pós-condições quando a execução do componente, função ou procedimento do módulo criptográfico for realizada. As pré-condições e pós-condições podem ser especificadas por qualquer notação que seja suficientemente detalhada para explicar o comportamento do componente, função ou procedimento do módulo criptográfico.

REQUISITO III.11.14: [FIPS 140-2, 4.10] A documentação deve especificar uma prova informal da correspondência entre o projeto do módulo criptográfico e a especificação funcional.

3.12 Mitigações de ataques

Esta seção apresenta requisitos técnicos referentes a ataques que não são considerados invasivos ao módulo criptográfico. Tais ataques podem ser considerados para módulos criptográficos que encontram-se 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.12.1: [FIPS 140-2, 4.11] A documentação do módulo criptográfico deve especificar quais os tipos de ataques não invasivos são mitigados pelo módulo.

Nivel de Segurança 2

REQUISITO III.12.2: [FIPS 140-2, 4.11] O HSM deve ser capaz de mostrar evidências de violação depois uma tentativa (não invasiva) de mexer com o hardware do HSM.

Nivel de Segurança 3

REQUISITO III.12.3: [FIPS 140-2, 4.11] O HSM deve ser capaz de resistir qualquer tentativa (não invasiva) de mexer com o hardware do HSM na maneira de zeramento da memória do HSM caso houverá violação.

4 Requisitos de Gerenciamento

Os requisitos de gerenciamento referem-se a funcionalidades que devem estar disponíveis aos operadores do módulo criptográfico, permitindo-lhe 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

4.1 Gerenciamento do Hardware

4.1.1 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 deve 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;

4.1.2 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 de manutenção o qual terminado, coloque-o em estado de operação segura;

4.1.3 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 (HSM) é ativado.

4.1.4 Controle de ativação M de N

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

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

DEFINICÃO IV.1.3: "M de N" é um método de segurança para as chaves criptográficas do HSM. No mínimo "M" pessoas das "N" cadastradas devem estar presentes para o acesso as operações do sistema de HSM.

Esse método previne ações unilaterais dos operadores do HSM através da divisão da senha de acesso ao HSM em "N" partes. A chave só será reconstruída se no mínimo "M" partes de "N" prover a sua senha (parte) individual.

Um exemplo comumente usado nesse caso é o de "3 de 5", onde a senha de acesso ao HSM é dividida em 5 partes e no mínimo, necessitará de 3 dessas 5 pessoas para acessar o HSM.

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

4.1.5 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.

4.2 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, aos seguintes aspectos:

- Possuir interface gráfica em idiomas português do Brasil ou em 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 meio de autenticação ;
- Permitir a reinicialização dos módulos criptográficos.

4.3 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 HSM:

- 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; e
    - Permissões.
- Recuperar parâmetros sobre uma determinada chave criptográfica assimétrica, tais como:
    - Algoritmo;
    - Expoente público (RSA);
    - Módulo (RSA);
    - Tamanho da chave; e
    - Permissões.

4.4 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 HSM:

- Exportar chave criptográfica assimétrica pública do módulo criptográfico;
- Gerar cópia de segurança da chave criptográfica assimétrica privada do módulo criptográfico;

5 Requisitos Interoperabilidade

Os requisitos 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.

5.1 Requisitos Gerais de Interoperabilidade

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

- Microsoft CryptoAPI;
- PKCS#11 v. 2.11;
- JCE/JCA;
- Interface própria; e
- 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; e
b. Microsoft Windows 2000 e versões superiores.

5.1.1 Requisitos gerais

REQUISITO V.1.3: 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, Exponente 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, Exponente público, Exponente 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.
- *Assinar* especificando os componentes de chaves assimétricas privadas em texto claro.
- *Verificar* especificando os componentes de chaves assimétricas públicas em texto claro.

REQUISITO V.1.4: A implementação da interface nativa deve suportar os algoritmos criptográficos descritos na seção 2.1.1, “Algoritmos Criptográficos Obrigatórios”.

5.1.2 Requisitos sobre CryptoAPI

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 suportar, no mínimo, as seguintes chamadas:

- *CPAcquireContext* 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*;

REQUISITO V.1.7: A implementação de MS CryptoAPI deve suportar os algoritmos criptográficos descritos na seção 2.1.1, "Algoritmos Criptográficos Obrigatórios".

5.1.3 Requisitos sobre PKCS#11

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

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

- *GenerateKey* especificando templates de chaves simétricas
- *GenerateKeyPair* especificando templates de chaves assimétricas
- *Sign* para realizar assinar de um conteúdo
- *Verify* para verificar a assinatura de um conteúdo
- *CreateObject* especificando templates de chaves assimétricas (no mínimo chave pública)
- *DestroyObject* especificando o *handle* do objeto

REQUISITO V.1.10: A implementação PKCS#11 deve suportar os algoritmos criptográficos descritos na seção 2.1.1, "Algoritmos Criptográficos Obrigatórios".

5.1.4 Requisitos sobre Java Cryptographic Extension (JCE)

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

REQUISITO V.1.12: A documentação deve especificar os componentes de software implementados do provedor de serviço criptográfico.

REQUISITO V.1.13: A documentação deve especificar o processo de configuração e instalação do provedor de serviço criptográfico.

REQUISITO V.1.14: Se aplicável 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.1.15: 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.1.16: A implementação JCE deve suportar os algoritmos criptográficos descritos na seção 2.1.1, “Algoritmos Criptográficos Obrigatórios”.

RECOMENDAÇÃO V.1.1: De forma opcional, sugere-se que o provedor de serviço criptográfico seja assinado por uma chave privada ligada a um certificado digital reconhecido no âmbito ICP-Brasil.

5.1.5 Requisitos sobre OpenSSL

REQUISITO V.1.17: Quando aplicável o módulo criptográfico deve ser capaz de fazer as seguintes operações utilizando chamadas da API do OpenSSL:

- *Gerar Chaves Simétricas* especificando templates em texto claro de chaves simétricas
- *Gerar Par de Chaves* especificando templates em texto claro de chaves assimétricas com os componentes *Módulo, Expoente público, tamanho em bits etc.*

- *Gerar Objeto de chaves* especificando templates de chaves assimétricas (no mínimo chave pública) com os componentes *Módulo, Expoente público, Expoente Privado em forma reduzida ou em forma de TRC (Teorema de Resto Chinês)*

REQUISITO V.1.18: A implementação da OpenSSL deve suportar os algoritmos criptográficos descritos na seção 2.1.1, “Algoritmos Criptográficos Obrigatórios”.

5.2 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.

6 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 eletro-eletrônicos.

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 material eletro-eletrônico dispensado.

Em alguns países fora do continente europeu há regras e normas compatíveis, semelhantes ou derivadas da RoHS e WEEE que também visam a preservação da saúde humana e do meio-ambiente em relação a substâncias nocivas pelo contato ou exposição prolongadas.

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: O equipamento deve estar em conformidade com as regras da Diretiva da União Européia (2002/95/EC) de Restrição a Substâncias Nocivas (RoHS –

Restriction to the use of Hazardous Substances), respeitando as restrições impostas às substâncias citadas.

RECOMENDAÇÃO VI.2: A parte interessada deve 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: A parte interessada deve apresentar certificado dos fornecedores de materiais, peças, componentes ou partes integrantes do equipamento final atestando a conformidade com a diretiva da RoHS.

7 Referências Bibliográficas

[1] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). Federal Information Processing Standards Publication – Security Requirements for Cryptographic Modules – FIPS PUB 140-2. US Government Printing Office, Washington, May 25, 2001.

[2] RSA LABORATORIES – PKCS#11: CRYPTOGRAPHIC TOKEN INTERFACE STANDARD.

[3] RSA LABORATORIES. PKCS #7: **Cryptographic Message Syntax Standard.** Version 1.5. 1993. 30p. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc>. Acesso em: 30.jan.2006.

[4] 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.

[5] 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.

[6] 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.

[7] 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. 21 p.

[8] COMITÊ GESTOR DA ICP-BRASIL. Resolução N° 41, de 18 de abril de 2006: Requisitos Mínimos para as Políticas de Certificados na Infra-estrutura de Chaves Públicas Brasileira (ICP-BRASIL). Brasília: ICP-BRASIL, 2006. 20 p.

[9] COMITÊ GESTOR DA ICP-BRASIL. DOC ICP-01.01 versão 1.0, de 18 de maio de 2006: Padrões e Algoritmos Criptográficos da Infra-estrutura de Chaves Públicas Brasileira (ICP-BRASIL). Brasília: ICP-BRASIL, 2006. 4 p

[10]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.

[11]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.

[12] 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.

[13]RSA LABORATORIES. PKCS #7: Cryptographic Message Syntax Standard. Version 1.5. 1993. 30p. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc>. Acesso em: 30.jan.2006.

[14]RSA LABORATORIES. PKCS #1: RSA Cryptography Standard. Version 2.1. 2002. 61p. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf>. Acesso em: 30.nov.2006.

[15]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.

[16]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.

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

[18] 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.

[19] NIST. FIPS 46-3 – Data Encryption Standard (DES). 1999. 26p.

[20] NIST. FIPS 140-2 – Security Requirements for Cryptographic Modules. 2002.

[21] NIST. Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules. 2004.

[22] NIST. FIPS 180-2 – Secure Hash Standard (SHS) com nota de mudança 1. 2004.

[23] NIST. FIPS 186-2 – Digitial Signature Standard (DSS) com nota de mudança 1. 2001. 76p.

[24] NIST. FIPS 197 – Advanced Encryption Standard (AES). 2001. 51p.

[25] NIST. FIPS 198 – The Keyed-Hash Message Authentication Code (HMAC). 2002

[26] NIST. FIPS Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. 2005.

[27] NIST. FIPS Special Publication 800-38C - Counter with Cipher Block Chaining-Message Authentication Code (CCM). 2004.

[28] ANSI X9.17 – Key Management. Descontinuado, mas o gerador de números pseudo aleatórios baseado em cifra de bloco ainda é válido.

[29] ANSI. X9.31 – Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA). 1998.

[30] ANSI. X9.62 – Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA). 2005

[31] ANSI. X9.80 – Prime Number Generation, Primality Testing, and Primality Certificates. 2005.

[32] ANSI. X9.81-1 – Random Number Generation Part 1: Overview and Basic Principles

[33] 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 .

[34] FREQUENTLY ASKED QUESTIONS ON HAZARDOUS SUBSTANCES IN ELECTRICAL AND ELECTRONIC EQUIPMENT (RoHS) AND DIRECTIVE 2002/96/EC WASTE ELECTRICAL AND ELETRONIC EQUIPMENT DIRECTIVE (WEEE).

[35] CALIFORNIA ROHS WORKSHOP. CALIFORNIA EPA DEPARTMENT OF TOXIC SUBSTANCES CONTROL; HAZARDOUS WASTE MANAGEMENT PROGRAM; REGULATORY AND PROGRAM DEVELOPMENT DIVISION.

[36] IEC CISPR 22

[37] IEC CISPR 24

[38] CODE OF FEDERAL REGULATIONS 47 Part 15

[39] IEC 50