LEA

Material Técnico a ser depositado para Homologação de Módulos de Segurança Criptográficos no âmbito da ICP-Brasil

São Paulo, 18 de junho de 2007.

Título	Material Técnico a ser depositado para Homologação de Módulos de Segurança Criptográficos no âmbito da ICP-Brasil
Versão	versão 1.0 preliminar 2
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

Datasheet	Especificação detalhada e completa de um determinado componente eletrônico
Norma	Documento que define regras, princípios, conceitos e padrões de conduta das atividades internas do LEA.
Procedimento	Documento que define procedimentos de execução das atividades internas do LEA.

Lista de Acrônimos

API	Application Programming Interface
CI	Circuito Integrado
CSP	Cryptographic Service Provider
FIPS	Federal Information Processing Standards
ICP-Brasil	Infra-estrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
JCA	Java Cryptography Architecture
JCE	Java Cryptography Extension
LEA	Laboratório de Ensaios e Auditoria.
NCSP	Non-Cryptographic Service Provider
NID	Número de Identificação do Documento
NH	Nível de Homologação
NS	Nível de Segurança
PC/SC	Personal Computer / Smart Card
PKCS	Public Key Cryptography Standards
RND	Random Number Generator
SCL	Sistema de Componentes da Leitora
SDK	Software Development Kit
SP	Service Provider
JRE	Java Runtime Enviroment
NIST	National Institute of Standards and Technology
MCT	Manual de Condutas Técnicas

1 Introdução

O objetivo deste documento é detalhar o material e a documentação técnicos a serem depositados pela parte interessada junto ao LSI-TEC/LEA para a realização dos processos de homologação de Hardware Security Modules (HSMs) no âmbito da ICP-Brasil, conforme estabelecido pelo MCT-X.

O material e documentação técnicos referidos são classificados em três categorias:

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

Três Níveis de Homologação (NH) distintos foram estabelecidos para HSMs

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

Para os NHs 2 e 3, a parte interessada pode depositar o código fonte de duas maneiras diferentes:

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

Também foram estabelecidos Três Níveis de Segurança (NS)

	NS	1	2	3
Controle de acesso	Role-Based			
	Identity Based			
Segurança física	Invólucro			
	Evidência			
	Resistência			
Garantia do projeto	Manuais			
	Código fonte			
	Modelo formal			

Tabela 1: Definição de Níveis de Segurança

A parte interessada opta pelo nível a ser homologado para cada um dos subitens (Controle de acesso, Segurança física e Garantia de projeto).

2 Material e documentação técnicos a serem depositados

A relação de materiais e documentação técnicos a serem depositados junto ao LSI-TEC/LEA

2.1 Componentes Físicos

Para os NHs 1, 2 e 3, os seguintes componentes físicos devem ser depositados junto ao LSI-TEC/LEA pela parte interessada:

- Hardware Security Module: Amostras nas quantidades definidas por este documento para cada modelo e/ou versão de HSM a ser submetido ao processo de homologação.
- Material de apoio: Caso o HSM submetido necessite de hardware de apoio como cartão inteligente, leitora ou token, serão necessários, no caso de:
  - Cartão inteligente: Amostras nas quantidades definidas por este documento a ser submetido ao processo de homologação.
  - Leitora de Cartão inteligente: Amostras nas quantidades definidas por este documento a ser submetido ao processo de homologação.
  - Token: Amostras nas quantidades definidas por este documento a ser submetido ao processo de homologação.

2.2 Documentação Técnica

2.2.3 Nível de Homologação 1

2.2.3.1 Manuais do produto

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

Requisito de depósito de manuais do produto	Manual
1	Instalação
2	Configuração
3	Operadores
4	Administrador (Security Officer)
5	Desenvolvedor
6	Integração
7	Importação de chaves

2.2.3.2 Documentação técnica específica

A parte interessada deve depositar ao LSI-TEC/LEA a seguinte documentação específica, aqui representada pela seção correspondente do MCT-X

MCT-X Seção 3.1 – Especificação do Módulo Criptográfico

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

MCT-X Seção 3.3 – Portas e Interfaces

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

MCT-X Seção 3.4 – Papeis serviços e autenticação

Documentação – Nível de segurança 1, 2, 3
Controle de acesso empregado pelo módulo
Mecanismo de autenticação (baseado em papel ou identidade)
Os tipos de dados de autenticação
Especificar os papéis autorizados suportados
Funcionalidades atribuídas ao papel de acesso “Usuário”
Funcionalidades atribuídas ao papel de acesso “Oficial de Segurança”
Funcionalidades atribuídas ao papel de acesso “Manutenção”
Serviços empregados pelo módulo
Entradas e saídas de serviços
Papéis de acesso autorizados no qual o serviço pode ser realizado
Serviços fornecidos sem autenticação
Especificar a força ou robustez dos mecanismos de autenticação

MCT-X Seção 3.5 – Modelo de Estado Finito

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

MCT-X Seção 3.6 – Segurança Física

Documentação
Especificar todos os componentes de hardware, software, firmware que estão contidos na fronteira criptográfica e protegidos pelos mecanismos de segurança física implementados.
Especificar quais mecanismos de segurança física estão implementados no módulo e seus respectivos componentes
Mecanismos de destruição de chaves criptográficas simétricas e assimétricas privadas e PCSs
Sensores para portas ou coberturas removíveis

MCT-X Seção 3.7 – Ambiente Operacional

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

MCT-X Seção 3.8 – Gerenciamento de chaves criptográficas

Documentação – Nível de segurança 1, 2, 3
Especificar todas as chaves criptográficas, seus componentes e PCS empregados pelo módulo
Especificar quais métodos são utilizados pelo módulo criptográfico para proteger chaves secretas, chaves privadas e PCS contra divulgação, modificação e substituição não autorizada.
Especificar quais métodos são utilizados pelo módulo criptográfico para proteger chaves públicas contra modificação e substituição não autorizada.
Especificar cada método de RNG empregado pelo módulo, seja ele aprovado ou não pelo padrão FIPS.
Especificar cada um dos métodos de geração de chaves criptográficas empregados pelo módulo (aprovados ou não pela família de padrões FIPS).
Especificar os métodos de atribuição de chaves empregados pelo módulo criptográfico (automático, manual ou combinação dos anteriores).
Especificar os métodos de importação e exportação de chaves criptográficas empregados pelo módulo (métodos aprovados ou não pela família de padrões FIPS).
Especificar os métodos de armazenamento de chaves criptográficas empregados pelo módulo.
Especificar os métodos de sobrescrita de chaves criptográficas com zeros binários que são empregados pelo módulo.

MCT-X Seção 3.9 – Interferência/Compatibilidade Eletromagnética

Documentação
Documentação comprovando conformidade do equipamento às normas de EMI/EMC para equipamentos de tecnologia da informação compatíveis com as normas reconhecidas internacionalmente
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
Documentação deve citar a qual órgão regulador o laboratório está credenciado.

MCT-X Seção 3.10 – Auto-testes

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

MCT-X Seção 3.11 – Garantia de projeto

Documentação – Nível de segurança 1
Manuais dos operadores
Documentação **– Nível de segurança 2**
Código fonte de firmware e outros componentes externos
Documentação **– Nível de segurança 3**
Modelo formal que descreva as regras e características da política de segurança
Especificar uma justificativa que demonstre a consistência e completude do modelo formal
Prova informal da correspondência do modelo formal e a especificação funcional
Especificar uma prova informal da correspondência entre o projeto do módulo criptográfico e a especificação funcional.

MCT-X Seção 3.12 – Mitigações de ataques

Documentação
Proteção contra ataques não invasivos
Proteção contra outros tipos de ataques

MCT-X Seção 4 – Gerenciamento do HSM

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

MCT-X Seção 5 – Interoperabilidade

Documentação
Especificação da capacidade de armazenamento

MCT-X Seção 6 – Restrição de Substâncias Nocivas

Documentação
Equipamento deve estar em conformidade com as regras da Diretiva da União Européia (2002/95/EC) de Restrição a Substâncias Nocivas (RoHS)
Documentação deve detalhar a conformidade do equipamento e de suas partes (materiais, peças, componentes, etc) com as diretrizes da RoHS, especificando a concentração das substâncias presentes dentro da proporção sugerida pela convenção RoHS
Certificado dos fornecedores de materiais, peças, componentes ou partes integrantes do equipamento final atestando a conformidade com a diretiva da RoHS

2.2.3.1 Documentação geral

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

- Aderência aos requisitos de segurança FIPS 140-2: Este documento deve ser gerado pela parte interessada, segundo modelo definido neste manual. Deve ser informado, para cada requisito de segurança definido no "Manual de Condutas Técnicas – Volume X", se esse requisito é atendido, descrevendo os detalhes técnicos necessários. Opcionalmente, para indicar que um dado requisito de segurança é atendido, podem ser inseridas referências aos demais documentos técnicos depositados;
- Aderência aos requisitos de gerenciamento: Este documento deve ser gerado pela parte interessada, segundo modelo definido neste manual. Deve ser informado, para cada requisito de gerenciamento definido no "Manual de Condutas Técnicas – Volume X", se este requisito é atendido, descrevendo os detalhes técnicos necessários. Opcionalmente, para indicar que um dado requisito de gerenciamento é atendido, podem ser inseridas referências aos demais documentos técnicos depositados;
- Aderência aos requisitos de interoperabilidade: Este documento deve ser gerado pela parte interessada, segundo modelo definido neste manual. Deve ser informado, para cada requisito de interoperabilidade definido no "Manual de Condutas Técnicas – Volume X", se esse requisito é atendido, descrevendo os detalhes técnicos necessários. Opcionalmente, para indicar que um dado requisito de interoperabilidade é atendido, podem ser inseridas referências aos demais documentos técnicos depositados;
- Aderência aos requisitos para restição de substâncias nocivas: Este documento deve ser gerado pela parte interessada, segundo modelo definido neste manual. Deve ser informado, para cada requisito de restrição de substâncias nocivas definido no "Manual de Condutas Técnicas – Volume X", se esse requisito é atendido, descrevendo os detalhes técnicos necessários.

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

2.2.4 Nível de Homologação 2

Adicionalmente aos documentos técnicos solicitados na seção 2.2.3, os seguintes itens devem ser depositados junto ao LSI-TEC/LEA pela Parte Interessada:

- Código fonte do componente PRNG *(Pseudo Random Number Generator);*
- Código fonte do componente de geração de chaves;
- Código fonte do componente de atribuição de chaves;
- Código fonte do componente de sobrescrita de chaves;
- Código fonte do componente de armazenamento de chaves;
- Código fonte do componente de importação/exportação de chaves e sementes;

2.2.5 Nível de Homologação 3

Adicionalmente aos documentos técnicos solicitados nas seções 2.2.3 e 2.2.4, os seguintes itens devem ser depositados junto ao LSI-TEC/LEA pela parte interessada:

- Código fonte embarcado: Relação de todo código fonte de software e/ou firmware embarcados no cartão inteligente. Caso utilize tecnologia *Java Card* e possua *applets* de funções criptográficas, fornecer o código fonte desses *applets*;

- Código fonte de apoio: Relação de todo código fonte de apoio relacionado às interfaces de programação (API), SDK (*Software Development Kits*), SP (*Service Providers*), CSP, ferramenta de gerenciamento e bibliotecas de software suportadas pelo módulo criptográfico.

2.3 Componentes em Software Executável

Para os NHs 1, 2 e 3, os seguintes componentes em softwares executáveis devem ser depositados junto ao LSI-TEC/LEA pela parte interessada:

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

3 Quantidades de material e documentação técnicos a serem depositados

A Tabela 2 apresenta os materiais e documentação técnicos a serem depositados pela parte interessada junto ao LSI-TEC/LEA referente ao processo de homologação de HSMs do tipo com interface PCI.

As quantidades de material e documentação técnicos apresentados na Tabela 2 devem seguir os seguintes critérios:

- Quanto aos componentes físicos: devem ser entregues ao LSI-TEC/LEA1 (uma) amostra para cada modelo e/ou versão de HSM do tipo com interface PCI a ser submetido ao processo de homologação;
    - Material de apio: no contexto do HSM entregue deve incluir seguinte material
        - Cartão inteligente: devem ser entregues ao LSI-TEC/LEA4 (quadro) amostras para cada papel de acesso ao HSM a ser submetido ao processo de homologação, no caso que controle de acesso é implementado por meio de cartão inteligente;
        - Leitora de cartão inteligente: devem ser entregues ao LSI-TEC/LEA, 1 (uma) amostra, no caso que controle de acesso é implementado por meio de cartão inteligente;
        - Token: devem ser entregues ao LSI-TEC/LEA, 4 (quadro) amostras para cada papel de acesso ao HSM a ser submetido ao processo de homologação, no caso que controle de acesso é implementado por meio de token;
- Quanto à documentação técnica:
    - Documentos impressos (Documentos Técnicos): devem ser entregues ao LSI-TEC/LEA em 3 (três) cópias de igual teor (por exemplo, três cópias impressas do manual de segurança do módulo criptográfico);

- Documentos eletrônicos (Documentos Técnicos): devem ser entregues ao LSI-TEC/LEA em 2 (duas) cópias de igual teor e armazenadas, obrigatoriamente, em 2 (duas) mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como documentos técnicos o manual de usuário, a política de segurança não proprietária, o manual da ferramenta de gerenciamento e código fonte);

- Quanto aos componentes em softwares executáveis: devem ser entregues ao LSI-TEC/LEA em 2 (duas) cópias de igual teor e armazenadas, obrigatoriamente, em 2 (duas) mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como componentes em softwares executáveis, a ferramenta de gerenciamento do módulo criptográfico e o CSP do módulo criptográfico).

Tabela 2: Quantidade de material e documentação técnicos a serem depositados

Requisito de depósito	Material e Documentação Técnicos a serem depositados pela parte interessada – NH 1
1	HSM do tipo com interface PCI (1 HSM)
2	Cartão inteligente (4 cartões por papel de acesso)
2	Leitora de cartão inteligente (1 leitora)
2	Token de acesso (4 tokens por papel de acesso)
3	PIN padrão
4	Documento de aderência aos requisitos (segurança, interoperabilidade, gerenciamento e funcionais)
5	Projeto de hardware, software e firmware
6	Política de segurança não proprietária
7	Manual de usuário e manual de instalação
8	Manuais das interfaces de programação (APIs) e bibliotecas de desenvolvimento
9	Manual da ferramenta de gerenciamento do cartão inteligente
10	Manual(is) de provedor(es) de serviço
11	Manual de comandos APDU suportados
12	Projeto de software de apoio
13	Relação de certificados obtidos
14	Outros documentos
Requisito de depósito	**Material e Documentação Técnicos a serem depositados pela parte interessada – NH 2**
15	Código fonte do componente PRNG *(Pseudo Random Number Generator);*
16	Código fonte do componente de geração de chaves;
17	Código fonte do componente de atribuição de chaves;
18	Código fonte do componente de sobrescrita de chaves;
19	Código fonte do componente de armazenamento de chaves;
20	Código fonte do componente de importação/exportação de chaves e sementes;
Requisito de depósito	**Material e Documentação Técnicos a serem depositados pela parte interessada – NH 3**
21	Código fonte embarcado
22	Código fonte de apoio
Requisito de depósito	**Componentes em software executável a serem depositados pela parte interessada – NH 1, 2 e 3**
23	Provedor(es) de serviço criptográfico
24	Ferramenta de gerenciamento do módulo criptográfico

25	Outras bibliotecas de software e/ou programas

4 Referências

[1] LABORATÓRIO DE ENSAIOS E AUDITORIA (LEA). **Norma de Elaboração de Documentos**. Versão 2.0. São Paulo: LEA, 2006. 22p.

[2] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 10520: Informação e documentação - citações em documentos: apresentação**. Rio de Janeiro: ABNT, 2002.

[3] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Manual de Condutas Técnicas – Volume X**: Detalhamento dos Requisitos Técnicos para Hardware Security Modules (*HSMs*) no âmbito da ICP-Brasil. Versão 1.0.