LEA

Procedimentos de Testes em

Módulos de Segurança Criptográficos

versão 1.0 preliminar 3

São Paulo, 18 de junho de 2007.

Título	Procedimentos de Testes em Módulos de Segurança Criptográficos
Versão	versão 1.0 preliminar 3
Data	18 de junho de 2007
Autor(es)	Mads Rasmussen
Classificação	Público

Sumário

Listas de Ilustrações

Lista de Figuras

Lista de Tabelas

Controle de Versão

Versão revisada	Data de emissão	Alterações realizadas

Glossário

Exemplos	Exemplos
ABNT	Associação Brasileira de Normas Técnicas
LEA	Laboratório de Ensaios e Auditoria.
NID	Número de Identificação do Documento
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.
RTF	*Rich Text Format*

Lista de Acrônimos

AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil

1 Introdução

Este documento tem por objetivo especificar os procedimentos de testes em equipamentos HSMs (Hardware Security Module) concedidos ao LEA. O propósito de uso de tais equipamentos é exclusivo ao estudos de funcionalidade, para auxiliar na escrita dos Manuais de Condutas Técnicas – Volumes X, XI e XII e, portanto, não fazem parte de qualquer processo de homologação.

Um HSM pode ser um componente de hardware (uma placa PCI) de um computador servidor ou um servidor "*stand alone*". A figura 1 apresenta os principais componentes de um servidor com HSM instalado.

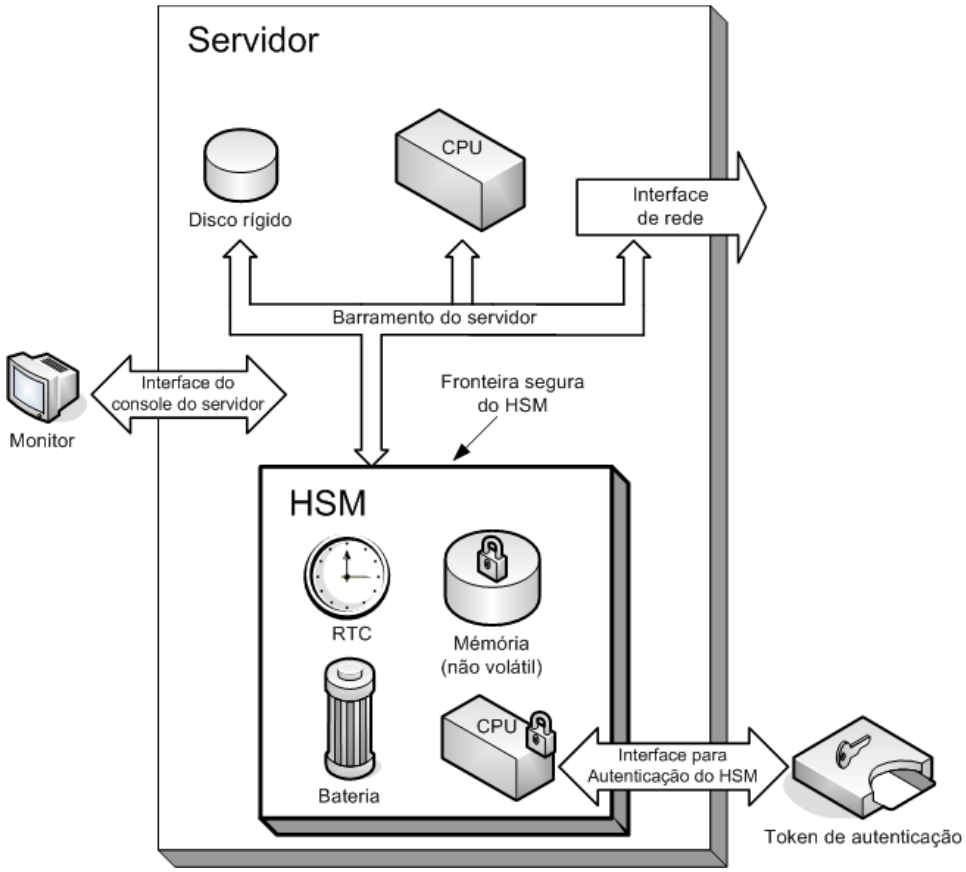

Figura 1: Principais componentes de um HSM

1.1 Precauções

A seguir é apresentada uma lista de precauções e cuidados que devem ser tomados durante a manipulação de um HSM:

- A interação com o servidor deverá ocorrer somente por meio de interface de comandos (*console*), ou interfaces específicas tais como, HTTPS, Socket, SSH etc.
- Como requisito de segurança física, o gabinete deve possuir mecanismos que destruam as informações no HSM em caso de violação física do gabinete;
- Em caso de falha de algum componente de hardware, o fabricante ou a empresa que disponibilizou o servidor deve ser contactada informando o problema ocorrido.

OBS**:** É desejável uma versão de teste do HSM com mecanismos de detecção de violação do gabinete, que não invalide o equipamento durante uma violação. O HSM deve ser instalado e configurado num ambiente de rede local isolada.

2 Testes de configurações

Esta seção apresenta procedimentos que devem ser realizados para verificação de funcionalidades no processo de configuração do HSM, realizado antes de entrar no estado de operação.

A execução dos procedimentos de testes desta seção é condição necessária para execução dos demais procedimentos.

2.1 Documentação

PROCEDIMENTO II.01.01: Verificar se a documentação especifica quais procedimentos de inicialização devem ser adotados antes de ativar o HSM.

PROCEDIMENTO II.01.02: Verificar se a documentação especifica a arquitetura do sistema.

PROCEDIMENTO II.01.03: Verificar se a documentação especifica as interfaces de comunicação que deverão ser utilizadas para estabelecer um canal de comunicação com o HSM, assim como, opções de configurações para tais interfaces.

PROCEDIMENTO II.01.04: Verificar se a documentação especifica quais componentes de hardware de interface com o usuário serão necessários para a ativação e configuração do HSM, tais como: cartões inteligentes, leitora de cartões inteligentes, teclado, mouse, etc.

PROCEDIMENTO II.01.05: Verificar se a documentação especifica quais componentes de software serão necessários para a ativação e configuração do HSM, tais como, navegador web, sistemas operacionais compatíveis, etc.

PROCEDIMENTO II.01.06: Verificar se a documentação especifica instruções de montagem e instalação física do servidor.

PROCEDIMENTO II.01.07: Verificar se a documentação especifica os perfis de acesso, assim como usuários e senhas utilizados por padrão na primeira inicialização do HSM para acesso e configuração do equipamento.

PROCEDIMENTO II.01.08: Verificar se a documentação especifica quais interfaces de administração estão disponíveis, como por exemplo, HTTPS.

PROCEDIMENTO II.01.09: Caso o HSM ofereça suporte a uma interface administrativa por meio de HTTPS, verificar se a documentação especifica os procedimentos para habilitação de certificado digital para uso com o SSL.

2.2 Configurações de rede e interfaces

PROCEDIMENTO II.02.01: Ativar o HSM conforme as instruções fornecidas e, monitorar o processo de configuração e registrar qualquer comportamento de erro, por exemplo, sinais sonoros ou mensagens no console do servidor. Quando o servidor oferecer suporte a uma interface de administração e/ou configuração via console, será necessário a conexão de um monitor e um teclado ao servidor. Por meio deste console poderão ser observadas mensagens de erros ou avisos produzidos pelo equipamento.

PROCEDIMENTO II.02.02: Após a ativação do HSM, verificar quais interfaces de configuração e/ou administração (console ou Web) encontram-se disponíveis, relacionando qual a função de cada interface e quais funcionalidades de configuração e/ou administração estão disponíveis. A interface console deve estar disponível após a inicialização correta do HSM, no entanto, a interface Web pode não estar disponível devido as configurações de endereço IP, Firewall ou ausência de certificado digital habilitado no servidor da aplicação Web.

PROCEDIMENTO II.02.03: Quando o HSM é entregue sem qualquer configuração de rede e a interface Web para administração do servidor não se encontra disponível, a configuração de endereço IP e Firewall para um primeiro acesso à interface de administração Web deve ser realizada. Utilizando os parâmetros de autenticação padrão (usuário e senha) fornecidos pelo fabricante, e por meio do console do HSM, realizar a configuração de endereço IP e Firewall conforme especificado na documentação fornecida.

PROCEDIMENTO II.02.04: Quando o HSM é entregue com configurações de fábrica que permitem o acesso direto a interface administrativa por meio de aplicação Web, não há necessidade de prévia configuração de endereço IP e Firewall do HSM. Utilizando os parâmetros de autenticação padrão (usuário e senha) fornecidos pelo fabricante, realizar acesso a interface administrativa por meio da aplicação Web disponível no HSM. Relacionar quais opções de administração estão disponíveis com uma breve descrição.

PROCEDIMENTO II.02.05: Por meio da interface administrativa, executar os procedimentos de inicialização e configuração do HSM de acordo com a documentação fornecida. Relacionar quais ativos podem ser guardados no HSM e os papéis de acesso que podem ser criados dentro do HSM com suas respectivas finalidades, permissões e

mecanismos de autenticação necessários, como por exemplo, cartões inteligentes ou tokens criptográficos. Observar, quando aplicável, a possibilidade de configuração de papéis de acesso do tipo M de N no HSM, relacionados com a operação ou administração do HSM. Neste caso, é definido um conjunto de N tokens de autenticação dos quais apenas M, onde M é menor ou igual a N, são necessários para realizar tarefas específicas.

2.3 Acesso no HSM por meio de APIs

PROCEDIMENTO II.03.01: Verificar o suporte de no mínimo uma das seguintes APIs para análise de acesso ao HSM:

- Microsoft CryptoAPI;
- PKCS#11 v. 2.11;
- JCE/JCA;
- OpenSSL Engine, se aplicável.

2.3.1 Requisitos Gerais

PROCEDIMENTO II.03.02: 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: módulo, expoente público, tamanho em bits, etc;

- *Gerar Objeto de chaves* especificando os componentes de chaves assimétricas (no mínimo chave pública) em texto claro. Por exemplo: módulo, expoente público, expoente privado 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; e
- *Verificar* os componentes de chaves assimétricas públicas em texto claro.

PROCEDIMENTO II.03.03: Verificar se a documentação que acompanha o HSM especifica o suporte aos algoritmos criptográficos descritos na seção 2.1.1, “Algoritmos Criptográficos Obrigatórios” do MCT-X por meio de interface nativa.

2.3.2 Requisitos sobre CryptoAPI

PROCEDIMENTO II.03.04: Verificar se a documentação que acompanha o HSM especifica a versão da implementação do MS CryptoAPI suportado, caso aplicável.

PROCEDIMENTO II.03.05: Verificar se a documentação que acompanha o HSM especifica se a implementação do MS CryptoAPI suportar as seguintes operações :

- *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; e
- *CryptVerifySignature* para verificação da assinatura após a importação da chave pública via *CryptImportKey.*

PROCEDIMENTO II.03.06: Verificar se a documentação que acompanha o HSM especifica o suporte aos algoritmos criptográficos descritos na seção 2.1.1, "Algoritmos Criptográficos Obrigatórios" do MCT-X, por meio de MS CryptoAPI.

PROCEDIMENTO II.03.07: Verificar se a documentação que acompanha o HSM descreve se o provedor de serviço criptográfico é assinado por uma chave privada ligada a um certificado digital reconhecido no âmbito ICP-Brasil.

2.3.3 Requisitos sobre PKCS#11

PROCEDIMENTO II.03.08: Verificar se a documentação que acompanha o HSM especifica o suporte a interface PKCS#11, incluindo sua versão.

PROCEDIMENTO II.03.09: Verificar se a documentação que acompanha o HSM especifica o suporte a seguintes chamadas de PKCS#11:

- *GenerateKey* especificando os *templates* de chaves simétricas;
- *GenerateKeyPair* especificando *templates* de chaves assimétricas;
- *Encrypt* especificando a chave e o texto a cifrar;
- *Decrypt* especificando a chave e o texto a decifrar;
- *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); e
- *DestroyObject* especificando o *handle* do objeto.

PROCEDIMENTO II.03.10: Verificar se a documentação que acompanha o HSM especifica o suporte aos algoritmos criptográficos descritos na seção 2.1.1, “Algoritmos Criptográficos Obrigatórios” do MCT-X por meio de interface PKCS#11.

PROCEDIMENTO II.03.11: Verificar na documentação que acompanha o HSM se o provedor de serviço criptográfico é assinado por uma chave privada ligada a um certificado digital reconhecido no âmbito ICP-Brasil.

2.3.4 Requisitos sobre *Java Cryptographic Extension* (JCE)

PROCEDIMENTO II.03.12: Verificar se a documentação que acompanha o HSM especifica a versão da máquina virtual Java a ser suportada pelo pacote de classes JCE.

PROCEDIMENTO II.03.13: Verificar se a documentação que acompanha o HSM especifica os componentes de software implementados do provedor de serviço criptográfico.

PROCEDIMENTO II.03.144: Verificar se a documentação que acompanha o HSM especifica o processo de configuração e instalação do provedor de serviço criptográfico.

PROCEDIMENTO II.03.15: Verificar se a documentação que acompanha o HSM especifica os serviços criptográficos implementados no provedor de serviço criptográfico que não estejam na especificação JCE.

PROCEDIMENTO II.03.16: Verificar se a documentação que acompanha o HSM informa detalhes sobre o uso do provedor de serviço criptográfico como API no formato Javadoc com trechos de código-fonte.

PROCEDIMENTO II.03.17: Verificar se a documentação que acompanha o HSM especifica o suporte aos algoritmos criptográficos descritos na seção 2.1.1, "Algoritmos Criptográficos Obrigatórios" do MCT-X por meio de interface JCE.

PROCEDIMENTO II.03.18: Verificar se a documentação que acompanha o HSM descreve se o provedor de serviço criptográfico é assinado por uma chave privada ligado a um certificado digital reconhecido no âmbito ICP-Brasil.

2.3.5 Requisitos sobre OpenSSL

PROCEDIMENTO II.03.19: Verificar na documentação que acompanha o HSM se o módulo criptográfico é 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 privada em forma reduzida ou em forma de TRC (Teorema de Resto Chinês)
- Cifrar
- Decifrar

- Assinar
- Verificar assinatura

PROCEDIMENTO II.03.20: Verificar se a documentação que acompanha o HSM especifica o suporte aos algoritmos criptográficos descritos na seção 2.1.1, “Algoritmos Criptográficos Obrigatórios” do MCT-X por meio de interface OpenSSL.

2.4 Funcionalidades do HSM

PROCEDIMENTO II.04.01: Verificar se a documentação que acompanha o HSM especifica o algoritmo utilizado para gerar números aleatórios.

PROCEDIMENTO II.04.02: Verificar se a documentação que acompanha o HSM especifica a maneira de ter acesso ao chave privada, seja por token USB, chaves fornecidas por meio de PED, cartão inteligente ou outro meio.

PROCEDIMENTO II.04.03: Verificar se a documentação que acompanha o HSM especifica quais utilitários são incluídos para gerenciar e testar as funcionalidades do HSM.

PROCEDIMENTO II.04.04: Verificar se a documentação que acompanha o HSM especifica o tipo de autenticação utilizado no HSM e se é possível utilizar autenticação M-de-N.

PROCEDIMENTO II.04.05: Verificar se a documentação que acompanha o HSM especifica o tamanho das chaves ICP como tamanho das chaves RSA.

PROCEDIMENTO II.04.06: Verificar se a documentação que acompanha o HSM especifica o desempenho de processos críticos como geração de números aleatórios, geração de chaves RSA, assinar com chave privada e cifrar com chave pública.

PROCEDIMENTO II.04.07: Verificar se a documentação que acompanha o HSM especifica a capacidade de armazenamento disponível no HSM.

PROCEDIMENTO II.04.08: Verificar se a documentação que acompanha o HSM especifica o suporte ao *backup* e *recovery* de chaves.

2.5 Configurações de logs e estatísticas

PROCEDIMENTO II.05.01: Por meio da interface administrativa correspondente, verificar o menu de configuração de logs do HSM, observando quais informações podem ser armazenadas em registros de log e como são visualizadas. Configurar o HSM para gerar e armazenar todos os possíveis registros de log.

PROCEDIMENTO II.05.02: Por meio da interface administrativa correspondente, quando aplicável, verificar como são apresentadas as informações sobre a estatística emitidos pelo HSM, seja por meio de registros de logs ou por meio de gráficos.

2.6 Testes de segurança física

PROCEDIMENTO II.06.01: Verificar se a documentação que acompanha o HSM especifica qualquer sensor de violação física.

PROCEDIMENTO II.06.02: Verificar se a documentação que acompanha o HSM especifica os sensores de violação física externos e tenta ativa-los para testar o funcionamento. O HSM deve apagar as chaves contidas.

OBS: Existem testes em HSMs que podem ser intrusivos e danificar o equipamento. Os fabricantes podem sugerir alguns testes específicos que eles conhecem sobre equipamento próprio.

2.7 Verificação de estado do HSM

PROCEDIMENTO II.07.01: Por meio da interface administrativa correspondente, verificar o estado operacional do HSM, observando quais informações de estado ele apresenta, incluindo seus respectivos significados.

3 Referências

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

[2] **Instituto Nacional de Tecnologia da Informação.** < http://www.iti.gov.br/>. Acesso em 08.setembro.2005.

[3] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Resolução Nº 36, de 21 de Outubro de 2004. Aprova o Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no âmbito da ICP-Brasil.** Brasília: ITI, 21.Outubro.2004. 14p.

[4] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **INSTRUÇÃO NORMATIVA No. 02: Estabelece os procedimentos administrativos a serem observados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil.** Brasília: ITI, 13.Abril.2005.

[5] LABORATÓRIO DE ENSAIOS E AUDITORIA (LEA). **Procedimento de Preenchimento dos Livros-Ata dos Níveis 3, 4, e 5 de Segurança**. Versão 1.0. São Paulo: LEA, 2005.

[6] LABORATÓRIO DE ENSAIOS E AUDITORIA (LEA). **Procedimento de Depósito de Material de Ensaio**. Versão 1.0. São Paulo: LEA, 2005.

[7] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Manual de Condutas Técnicas – Volume I**: Detalhamento dos Requisitos Técnicos para Cartões Inteligentes (*Smart Cards*), Leitoras de Cartões Inteligentes e *Tokens* Criptográficos no âmbito da ICP-Brasil. Versão 1.1. Brasília: ITI, 2006. 66p.