

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO**

André Bereza Júnior

**Aprimoramento de um HSM para
Homologação na ICP-Brasil**

Trabalho de Conclusão de Curso submetido à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Bacharel em Ciência da Computação.

Jeandré Monteiro Sutil
Orientador

Prof. Ricardo Felipe Custódio, Dr.
Co-Orientador

Florianópolis, dezembro de 2009

Aprimoramento de um HSM para Homologação na ICP-Brasil

André Bereza Júnior

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Bacharel em Ciência da Computação e aprovada em sua forma final pelo Departamento de Informática e Estatística da Universidade Federal de Santa Catarina.

Prof. Luís Fernando Friedrich, Dr.

Coordenador do Curso

Banca Examinadora

Jeandré Monteiro Sutil

Prof. Ricardo Felipe Custódio, Dr.

Jean Everson Martina, M.Sc.

Túlio Cícero Salvaro de Souza, M.Sc.

Prof. Frank Augusto Siqueira, Dr.

Ofereço este trabalho aos meus pais, por terem me
fornecido condições de estudar e chegar aonde cheguei.

Agradecimentos

Agradeço aos meus amigos, porque se não fosse pela ajuda deles nos momentos mais difíceis, eu não teria concluído este trabalho e a minha graduação.

Um agradecimento especial ao professor Ricardo Felipe Custódio e ao LabSEC, por terem me acolhido e me ensinado praticamente tudo o que eu sei hoje.

Sumário

Lista de Figuras	x
Lista de Siglas	xi
Resumo	xii
Abstract	xiii
1 Introdução	1
1.1 Contextualização	1
1.2 Objetivo	1
1.3 Objetivos Específicos	2
1.4 Justificativa	2
1.5 Metodologia	2
1.6 Limitações do Trabalho	3
2 Fundamentos Criptográficos	4
2.1 Criptografia	4
2.1.1 Funções Resumo	5
2.1.2 Criptografia Simétrica	6
2.1.3 Criptografia Assimétrica	6
2.1.4 Segredo Compartilhado	7
2.2 Fatores de Autenticação	7
2.2.1 Smart Card	8

	vii
2.2.2 PIN	8
2.3 TLS/SSL	9
3 Módulo de Segurança Criptográfica	10
3.1 Sistema Embarcado	11
3.1.1 Ambiente Operacional	11
3.1.2 Persistência de Dados	13
3.1.3 Unidade de Gerência	14
3.1.4 Unidade de Segurança	15
3.2 Grupos de Gerenciamento	15
3.2.1 Administração	16
3.2.2 Auditoria	16
3.2.3 Operação	17
3.2.4 Funções Comuns a Todos os Perfis	17
3.3 Autenticação	18
3.4 Chaves Gerenciadas	18
3.5 Backup	19
3.6 Update de Firmware	19
3.7 Interfaces	19
3.7.1 Interfaces Físicas	20
3.7.2 Interfaces Lógicas	20
4 Homologação na ICP-Brasil	22
4.1 Órgão Homologadores	22
4.1.1 NIST	22
4.1.2 ITI	23
4.2 Níveis de homologação	24
4.2.1 Níveis de segurança de homologação	24
4.2.2 Níveis de segurança de física	25
4.3 Processo de Homologação	26

4.3.1	Entrega de documentação técnica e jurídica	26
5	Requisitos do MCT 7	31
5.1	Descrição	31
5.2	Proteção das chaves	33
5.2.1	Proteção física	33
5.2.2	Proteção lógica: uso indevido	34
5.2.3	Proteção lógica: algoritmos aprovados FIPS	35
5.2.4	Proteção lógica: exportação de chaves	35
5.2.5	Proteção lógica: sobrescrita com zeros	36
5.3	Documentação	37
5.4	Usabilidade	38
5.5	Interoperabilidade	39
5.6	Funcionalidades	39
5.6.1	Operação	40
5.6.2	Auto-testes	40
6	Implementação	42
6.1	Modo de Segurança	42
6.2	Auto-Testes	42
6.2.1	OpenSSL FIPS	43
6.2.2	Unidade de Segurança	44
6.2.3	Integridade do Firmware	44
6.2.4	Energização	46
6.2.5	Importação de Firmware	47
6.3	Estados do Módulo	48
6.3.1	Estado Operacional	48
6.3.2	Estado de Erro	48
6.4	Segregação de Dados	49
6.5	Nível Crítico do Espaço em Disco	50

7	Considerações Finais	51
	Referências	53
A	Etapas do Processo de Homologação	57
B	Diagramas de Estados	59
B.1	Diagrama Geral de Estados	59
B.2	Diagrama de Inicialização e Gerência de Perfis	61
B.3	Diagramas de Geração e Uso de Chaves	62
B.4	Diagramas relacionados ao Esquema de Backup	63

Lista de Figuras

A.1	Fluxograma do Processo de Homologação	58
B.1	Diagrama de estados do ASI-HSM	60
B.2	Diagrama de estados detalhando a inicialização e criação dos perfis do ASI-HSM	61
B.3	Diagrama de estados detalhando a criação de chaves do ASI-HSM. . .	62
B.4	Diagrama de estados detalhando a liberação e uso de chaves gerenciadas pelo ASI-HSM.	62
B.5	Diagrama de estados detalhando a configuração do ASI-HSM como unidade de backup.	63
B.6	Diagrama de estados detalhando a importação de chaves de backup. . .	63
B.7	Diagrama de estados detalhando a geração de backups de um ASI-HSM em operação.	64
B.8	Diagrama de estados detalhando a restauração de backup em um ASI-HSM préconfigurado.	65

Lista de Siglas

AC	Autoridade Certificadora
AES	Advanced Encryption Standard
ASI-HSM	Advanced Security Initiative - Hardware Security Module
CA	Certificate Authority
CF	Compact Flash
CMVP	Cryptographic Module Validation Program
CSEC	Communications Security Establishment Canada
DES	Data Encryption Standard
EuroPKI	European PKI Workshop
HSM	Hardware Security Module
ICP	Infra-estrutura de Chaves Públicas
ICP-Brasil	Infra-estrutura de Chaves Públicas Brasileira
ICPEDU	Infra-estrutura de Chaves Públicas para Ensino e Pesquisa
IDtrust	Symposium on Identity and Trust on the Internet
ITI	Instituto de Tecnologia da Informação
LabSEC	Laboratório de Segurança em Computação - UFSC
LEA	Laboratório de Ensaios e Análise
MCT	Manual de Condutas Técnicas
MSC	Módulo de Segurança Criptográfica
NIST	National Institute of Standards and Technology
NSF	Nível de Segurança Física
NSH	Nível de Segurança de Homologação
PI	Parte Interessada
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RNP	Rede Nacional de Ensino e Pesquisa
RSA	Rivest-Shamir-Adleman
SSL	Secure Socket Layer
TLS	Transport Layer Security
UG	Unidade de Gerência
US	Unidade de Segurança

Resumo

Com o avanço da tecnologia e dos algoritmos criptográficos foi concebida a atual esquemática para segurança de documentos eletrônicos conhecida como infra-estrutura de chaves públicas (ICP), que tem como base o par de chaves criptográficas, conhecidas como chave pública e chave privada. A segurança de documentos eletrônicos se refere à autenticidade, integridade, confidencialidade e não-repúdio de dados em meio digital.

A rede de confiança de uma ICP é formada pelas Autoridades Certificadoras (AC) que a compõe, sendo que cada AC deve manter a sua chave privada em segurança, para que a confiabilidade dos certificados gerados por ela seja garantida.

A guarda da chave privada se tornou uma função crucial para manter a ICP íntegra, para isso foi realizado este estudo procurando aprimoramentos possíveis em um Módulo de Segurança Criptográfica (HSM da sigla em inglês), que é um equipamento fabricado especialmente para este fim.

Para que um HSM seja utilizado na Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), ele deve estar em conformidade com o que esta instituição requer no que se refere a segurança das chaves contidas no HSM, ou seja, ele deve estar homologado nesta instituição. Os aprimoramentos no HSM terão como alvo a homologação na ICP-Brasil.

Palavras chave: Homologação ICP-Brasil, Módulo de Segurança Criptográfica, Infra-estrutura de Chaves Públicas, Criptografia Assimétrica.

Abstract

With the technological advance of cryptographic algorithms, was conceived the current organization to the security of electronic documents known as public key infrastructure (PKI), which base relies on the pair of cryptographic keys, known as public key and private key. The security of electronic documents refers to the authenticity, integrity, confidentiality and non-repudiation of data.

The web of trust of an PKI is formed by the Certificate Authorities (CA) that compose her, and every CA must maintain his private key in safety, to maintain the trust of the certificates generated by her.

The keep of the private key has become a crucial function to maintain the integrity of the PKI, for that was performed an study looking for possible improvements in an Hardware Security Module (HSM), which is an equipment made especially to this end.

To use an HSM in the Brazilian Public-Key Infrastructure (ICP-Brasil), it must be in concordance with the requirements of this institution regarding the security of the keys contained in the HSM, it must be approved in this institution. The improvements in the HSM will target the approval of ICP-Brasil.

Palavras chave: ICP-Brasil Homologation, Hardware Security Module, Public Key Infrastructure, Asymmetric Cryptography.

Capítulo 1

Introdução

O HSM é um dos componentes utilizados na gerência de uma AC, sendo composto por várias funções que vão desde a escrita de chaves criptográficas em disco até a proteção física do equipamento.

1.1 Contextualização

Uma das únicas soluções nacionais para Módulos de Segurança Criptográfica foi desenvolvida em conjunto pela empresa Kryptus, fabricante de hardwares criptográficos, e pelo LabSEC que foi o responsável pela implementação do software desse HSM, conhecido como ASI-HSM. O ASI-HSM faz parte do projeto ICPEDU, coordenado e financiado pela Rede Nacional de Ensino e Pesquisa (RNP), que é uma empresa pública ligada ao Ministério de Ciência e Tecnologia e sempre está incentivando o avanço tecnológico no Brasil.

1.2 Objetivo

Este trabalho tem como objetivo aprimorar uma solução de hardware criptográfico que já existe, para que ela possa ser homologada junto ao ITI. Dessa maneira este equipamento poderá ser utilizado no âmbito da ICP-Brasil.

1.3 Objetivos Específicos

O objetivo específico deste trabalho é o avanço da tecnologia nacional para criação de hardwares criptográficos, implementando melhorias e novas funcionalidades ao ASI-HSM, melhorias norteadas pelo ITI. Alguns aprimoramentos são:

- Melhorar a documentação de uso do ASI-HSM;
- Tornar o equipamento mais robusto;
- Colocar o ASI-HSM em nível competitivo com outros HSMs de mercado;
- Aumentar o valor do projeto ICPEDU, que passará a utilizar um HSM homologado ICP-Brasil.

1.4 Justificativa

Com a implementação de novas funcionalidades o ASI-HSM poderá ser utilizado na ICP-Brasil, pois é requisito do ITI que um HSM seja homologado para a utilização em seu âmbito. Como consequência da homologação o ASI-HSM receberá um selo de qualidade, assim outras instituições terão a comprovação do ITI de que o equipamento é seguro.

A padronização do equipamento também é um resultante da homologação e é muito importante para o usuário de um HSM, pois vários HSMs homologados no ITI tendem a ter funcionalidades e proteções bastante semelhantes, o que é algo natural quando se segue os mesmos critérios de conformidade.

1.5 Metodologia

O processo de homologação de um HSM é composto de várias partes distintas que o compõem. Existe a parte inicial que é bastante burocrática, na entrega

de documentação jurídica para iniciar o processo. Após isso passa para uma parte intermediária, que é a entrega de vários artefatos como a documentação técnica para a análise do ITI, documentação final (do usuário), HSMs a serem utilizados na análise e possivelmente seja necessária a implementação de funcionalidades. Por fim existe a etapa de ensaios e análise do equipamento, onde o HSM é submetido a vários testes de conformidade, visando comprovar as proteções afirmadas na etapa anterior.

Maiores detalhes sobre o processo de homologação podem ser encontrados no capítulo 4.

1.6 Limitações do Trabalho

Uma das limitações do trabalho é a participação no processo de homologação como um todo, pois neste trabalho não será tratada a questão jurídica no início do processo de homologação e também a parte final que são os ensaios de conformidade. Neste trabalho será abordada apenas a etapa intermediária, pois foi a que demandou maior esforço técnico e científico para a implementação de funcionalidades e confecção de documentação, visando tornar o ASI-HSM um equipamento que segue os requisitos do ITI.

Este trabalho foi desenvolvido como parte das atividades do LabSEC na fabricação do ASI-HSM. O LabSEC é responsável pela implementação do software do ASI-HSM, sendo esta outra limitação do trabalho, pois não trataremos com muitos detalhes as questões relacionadas ao hardware do equipamento.

Capítulo 2

Fundamentos Criptográficos

Com o avanço tecnológico e a valorização dos documentos eletrônicos, a segurança em computação ganhou mais espaço no cenário tecnológico/computacional. Para evitar o roubo de informações, mensagens e documentos, foram criados meios de se garantir a confidencialidade dos mesmos, mas nada disso seria possível sem a união dos métodos computacionais com a matemática. Esta união é estudada na criptografia, que significa escrever algo de forma escondida.

Os métodos matemáticos implementados pelas funções criptográficas não conseguem esconder a informação com perfeição, ou seja, é possível a descoberta dela, mas o tempo médio para a decifragem acaba se tornando proibitivo, avançando com facilidade a casa dos 100 anos. [SCH 96]

2.1 Criptografia

A criptografia é a ciência que estuda métodos de se esconder uma mensagem, de modo que ela possa ser descoberta posteriormente. Essa forma de esconder a mensagem não é como escrever algo com tinta invisível, pois a mensagem “escondida” ainda está visível, a diferença é que está escrita de uma maneira que não faz nenhum sentido. Esse processo é chamado cifragem de dados. [SCH 96]

Não faria nenhum sentido cifrar um dado e não deixar a possibilidade de

decifrá-lo depois, seria muito mais fácil deletar o arquivo ou não enviar a mensagem, dependendo do contexto. Para realizar as operações de cifrar e decifrar se faz uso do que chamamos de chave criptográfica, que é uma seqüência de bits capaz de cifrar o arquivo e decifrá-lo depois, colocando-o em seu estado original.

Existem vários tipos de algoritmos para cifrar e decifrar dados, alguns utilizando mais de uma chave criptográfica no processo.

2.1.1 Funções Resumo

As funções de resumo são conhecidas como funções de HASH, e tem o objetivo de transformar uma seqüência de bits em outra seqüência de tamanho fixo. Essa função criptográfica não necessita de uma chave para ser realizada. Uma característica importante do HASH é que não é possível retornar ao documento (mensagem, arquivo, etc.) original tendo como entrada somente o HASH calculado, ou seja, é uma função de sentido único.[SCH 96]

A entrada do algoritmo é uma seqüência qualquer de bits, isso torna o domínio da função um conjunto muito grande, maior que o contra-domínio que é uma seqüência fixa de bits. Isso faz com que na maioria dos casos o HASH calculado seja menor que a seqüência de bits inicial.

Para um bom algoritmo de HASH, a ocorrência de uma alteração significativa em uma seqüência de bits não deve resultar em um HASH igual ao calculado antes da alteração. Existem formas de se prevenir isso com o que é conhecido como “efeito avalanche” empregado nos algoritmos. Esse efeito consegue dificultar a geração de um HASH igual a partir de duas seqüências diferentes de bits, essa coincidência de HASHs é conhecida como colisão.[SCH 96]

Não é possível evitar totalmente as colisões de HASH, visto que o conjunto de entradas é infinito e o conjunto de saídas é finito. Um bom algoritmo de HASH deve dificultar ao máximo essa colisão, pois é o máximo que eles podem fazer com qualquer tecnologia.

2.1.2 Criptografia Simétrica

Na criptografia simétrica a cifragem e decifragem de dados utilizam a mesma chave, que pode ser chamada de chave simétrica. O fato de ser usada apenas uma chave para as duas operações leva a um sério problema que é o compartilhamento dessa chave. Sempre que um arquivo cifrado for enviado a alguém, a pessoa que o recebe deve ter posse da chave simétrica para visualizar o arquivo real, o problema está em como essa chave será compartilhada. Qualquer meio de se compartilhar a chave simétrica é suscetível a uma falha que faça com que o destinatário errado receba a chave, assim qualquer informação que foi cifrada com ela estará comprometida.[SCH 96]

Uma chave criptográfica não pode ser vulnerável a ataques de força bruta, onde o adversário tenta decifrar um documento usando todas as combinações possíveis de chave, geralmente se baseando em palavras de dicionário. Uma das características de uma boa chave é aquela que dificulta este tipo de ataque, isso é definido pelo tamanho da chave, que torna o conjunto de chaves possíveis muito grande ou pela imprevisibilidade (aleatoriedade) da chave gerada. [SCH 96]

2.1.3 Criptografia Assimétrica

Para resolver o problema do compartilhamento de chaves na criptografia simétrica, foram criados algoritmos de criptografia assimétrica, onde duas chaves são envolvidas no processo de cifragem e decifragem dos dados. [SCH 96]

Uma das chaves fica de posse do usuário dono do par de chaves e a outra chave é distribuída livremente, são conhecidas como chave privada e chave pública respectivamente. Os dados cifrados por uma das chaves só podem ser decifrados pela outra chave do par, mas não é possível derivar uma chave a partir da outra.

A chave privada é usada para determinar a autenticidade de um documento, cifrando o HASH do documento com a chave privada, assim o receptor do documento pode decifrar o HASH com a chave pública e conferir se está correto. A chave pública é usada para garantir a confidencialidade de um documento, onde o emissor cifra o documento com a chave pública do receptor, dessa maneira somente o receptor poderá

decifrar o documento. [SCH 96]

Nada impede que a criptografia simétrica e assimétrica sejam usadas em conjunto, como já acontece em vários protocolos como o TLS/SSL, melhor descrito na seção 2.3.

2.1.4 Segredo Compartilhado

Por vezes é necessário que mais de uma pessoa autorize a realização de uma tarefa, para isso o método do segredo compartilhado pode ser utilizado. Neste método uma chave criptográfica (o segredo) é dividida em várias partes e distribuída para n indivíduos.

Existem várias implementações do segredo compartilhado, mas a que trataremos neste trabalho é o esquema (t, n) , tal que t é igual ao número de indivíduos necessários para decifrar o segredo, n é o número de indivíduos que possuem uma parte do segredo, e $1 \leq t \leq n$.

Em um método de segredo compartilhado seguro, um indivíduo com $n-1$ partes do segredo tem a mesma quantidade de informação a respeito do segredo que uma pessoa com 0 partes.[SCH 96]

2.2 Fatores de Autenticação

Autenticar-se significa provar que você é quem diz ser. Existem várias maneiras de se realizar essa prova, como a autenticação por prova de posse (cartão de crédito, smart card), por senha (PIN), biometria (impressão digital, leitura da retina), terceira parte (certificado digital).

Neste trabalho é dada ênfase aos métodos de autenticação por prova de posse de um Smart Card e prova de conhecimento do PIN, pois estes são os métodos utilizados por um indivíduo que queira se autenticar no ASI-HSM.

2.2.1 Smart Card

Vários tipos de smartcards estão disponíveis no mercado, como cartões *contactless*, cartões *contact* e os cartões criptográficos. Neste estudo é abordado os cartões criptográficos *contact*, onde o contato do cartão com a leitora de smartcards é necessário.

Um cartão criptográfico difere dos cartões normais pela sua capacidade de gerar pares de chaves criptográficas e a utilização de algoritmos de criptografia simétrica. Neste estudo é abordado o cartão StarCos® SPK 2.3, por ser o único cartão ao qual o ASI-HSM dá suporte. Este cartão consegue realizar a geração de chaves RSA de até 1024 bits e cifrar dados com os algoritmos RSA, DES e 3DES.

Na geração de um perfil¹ para um indivíduo que portará o cartão, o smartcard faz a geração de um par de chaves RSA e exporta a chave pública para o HSM. O HSM devolve para o smartcard o certificado digital do usuário, correspondente à chave pública gerada. A chave privada RSA do indivíduo é cifrada com o algoritmo simétrico 3DES, e a chave usada para alimentar o algoritmo é um PIN escolhido pelo usuário.

Todo usuário faz parte de um grupo que detém a posse das partes de um segredo compartilhado. Essas partes do segredo ficam armazenadas no HSM, cifradas com a chave pública do usuário. No momento da autenticação de um perfil, a parte cifrada do segredo compartilhado é entregue para o smartcard, que é o único capaz de decifrá-la. Lembrando que para fazer uso da chave privada do usuário, é necessário decifrá-la com o PIN.

2.2.2 PIN

O PIN é uma forma de autenticação bastante comum, principalmente nos bancos, sendo consistido de caracteres numéricos.

No nosso estudo o PIN é responsável pela liberação para uso da chave privada RSA de um smartcard, decifrando-a com o algoritmo simétrico 3DES. Mais

¹A geração de perfis e usuários do ASI-HSM está descrita na seção 3.2

detalhes da operação estão na seção 2.2.1.

2.3 TLS/SSL

O TLS/SSL, é um protocolo de comunicação segura entre um cliente e um servidor. O cliente é aquele que requisita a conexão.

A comunicação é segura porque ela garante a autenticidade e confidencialidade dos dados. O estabelecimento da conexão TLS/SSL se dá em três etapas.

A primeira fase é a escolha de quais algoritmos serão usados na conexão. O cliente requisita a conexão com o servidor e informa quais algoritmos criptográficos ele suporta. Dessa lista fornecida pelo cliente, o servidor escolhe o algoritmo mais forte que ele também suporta, informando o cliente da decisão.

A segunda fase é a de autenticação e troca de chaves. O servidor envia o seu certificado digital para o cliente, assim o cliente pode verificar se o servidor é quem diz ser, garantindo a autenticidade. O cliente gera um número aleatório que será a chave da conexão, cifra esse número aleatório com a chave pública do servidor (contida no certificado digital) e envia para o servidor. Neste momento apenas o servidor e o cliente tem a posse do número aleatório.

Na terceira fase, o número aleatório gerado na segunda fase será usado para cifrar os dados que trafegarão entre o cliente e o servidor, estabelecendo assim um túnel de comunicação segura, garantindo a confidencialidade.

Capítulo 3

Módulo de Segurança Criptográfica

Neste capítulo será apresentado o ASI-HSM e suas funcionalidades. O ASI-HSM foi o módulo de segurança criptográfica depositado no ITI como objeto de homologação, bem como suas interfaces de administração e comunicação.

O ASI-HSM é um módulo interessante de se realizar o estudo, pois é um dos únicos HSMs produzidos atualmente no Brasil. A maioria dos componentes utilizados na sua fabricação são importados, mas a fabricação do ASI-HSM e o desenvolvimento de seus softwares de gerência são produto nacional, todos implementados pelo LabSEC e pela Kryptus.

Ao longo do desenvolvimento do ASI-HSM vários protocolos foram publicados pela equipe de desenvolvimento do LabSEC, em artigos, dissertações de mestrado e trabalhos de conclusão de curso. Algumas publicações foram realizadas em grandes congressos como o IDtrust¹ e o EuroPKI². Isso mostra que os protocolos do ASI-HSM são abertos e a sua segurança, confiabilidade e bom funcionamento podem ser verificados.

Foi atribuída bastante importância para a função de auditoria do ASI-HSM. A auditoria é essencial para que o usuário do módulo saiba que uma operação foi

¹A publicação no IDtrust referente aos protocolos de auditoria e backup do ASI-HSM pode ser encontrada na referência [dS 08].

²A publicação no EuroPKI referente aos protocolos de criação de grupos e geração de chaves no ASI-HSM pode ser encontrada na referência [MAR 07].

realizada, e quando foi realizada. Esta função é melhor descrita na seção 3.2.2.

3.1 Sistema Embarcado

A base do ASI-HSM embarcado é composta por um sistema operacional enxuto, contendo apenas as aplicações e bibliotecas necessárias para a execução dos seus softwares essenciais, já que o espaço para armazenamento de dados é pequeno, para fins de barateamento do equipamento.

3.1.1 Ambiente Operacional

O sistema operacional escolhido para embarcar no ASI-HSM foi o FreeBSD, sendo que atualmente é utilizada a versão 7.0-RELEASE. O hardware utilizado no equipamento se adaptou melhor ao FreeBSD, por isso ele foi o SO escolhido.

As aplicações contidas no SO podem ser divididas em dois grupos, o grupo das aplicações instaladas pela coleção de *ports* disponibilizadas pelo FreeBSD, e o grupo das aplicações desenvolvidas pelo LabSEC e pela Kryptus.³

3.1.1.1 Coleção de *ports*

A coleção de *ports* é uma maneira fácil de se instalar softwares que não estão inclusos na instalação padrão do FreeBSD. A instalação é realizada compilando o código fonte do software desejado. Se alguma dependência desse software não estiver instalada no SO, o *ports* faz a busca da dependência dentro de seu próprio sistema e realiza a instalação da mesma forma que o software dependente, de forma recursiva.

A vantagem da utilização do *ports* é que o software pode receber patches do fabricante (LabSEC ou Kryptus) e seu código executável gerado poderá ser auditado também pelo fabricante.

Os softwares mais importantes instalados via *ports* são:

³Por questões de simplicidade, as aplicações nativas ao SO não serão descritas, aplicações como *cp*, *fsck*, *reboot*, etc.

- CCID: driver genérico para um dispositivo de interface com Smart Cards.
- libusb: uma biblioteca para facilitar o uso de dispositivos USB, independente do Sistema Operacional. Dependência do PCSC-Lite e CCID.
- OpenCT: implementa drivers para diversas leitoras de Smart Card. Dependência do OpenSC.
- OpenSC: implementa drivers para Smart Cards.
- OpenSSH: aplicação usada para criação de túneis seguros TLS/SSL.
- OpenSSL: aplicação que contém uma grande biblioteca criptográfica para propósito geral.
- PCSC-Lite: aplicação que faz o acesso aos Smart Cards. Dependência do CCID.
- SQLite3: biblioteca de software que implementa uma engine SQL bastante leve (não precisa de servidor) e simples de utilizar.

3.1.1.2 Aplicações desenvolvidas pelos fabricantes

As aplicações desenvolvidas pelos fabricantes são compostas pela implementação do software que gerencia o ciclo de vida das chaves criptográficas, e drivers que possibilitam a comunicação com o hardware do HSM e com a Unidade de Segurança (ver seção 3.1.4).

As aplicações e bibliotecas são:

- cs5536smb: módulo dinâmico adicionado ao kernel durante a inicialização, responsável pela criação do dispositivo que representa a US.
- hsiapp: aplicação que faz uso de funções da US, como alterar a hora do sistema e alterar as mensagens do display.
- hsmdbSD: processo que faz a interface entre a UG e a US.

- `libkryptus`: Engine OpenSSL utilizada para a geração de números aleatórios, delegando a tarefa de geração à US.⁴
- `openhsm`: aplicação responsável pela gerência das chaves criptográficas e pelo gerenciamento de todo o HSM.
- `rng`: aplicação que fornece a semente utilizada no algoritmo de geração de números aleatórios.

3.1.2 Persistência de Dados

O ASI-HSM na sua versão atual, conhecida como AHX2L4, armazena seus dados em uma memória flash com capacidade de 1GB. Os dados são divididos em três partições físicas persistentes e uma partição volátil em memória.

A primeira partição física é a partição que contém o bootloader do SO e o sistema de arquivos inicial do HSM. Esta partição tem capacidade de 20MB e é responsável por carregar a partição volátil na memória, para então passar o controle do SO para essa partição, fazendo uso do `chroot` que é uma aplicação nativa do FreeBSD. Esta partição será posteriormente referenciada como partição inicial.

A partição volátil é conhecida como `hsmroot` e contém todas as aplicações citadas nas seções 3.1.1.1 e 3.1.1.2. Essas aplicações são executadas dessa partição volátil, pois elas não são alteradas durante a execução das funções do HSM. Esta partição tem capacidade de 25MB e posteriormente será referenciada como `hsmroot`.

Logo na inicialização do `hsmroot` a segunda partição física é montada no sistema de arquivos, mais especificamente no diretório `/cf`. Esta partição armazena os arquivos de configuração do `openhsm`, as chaves criptográficas gerenciadas pelo módulo e o arquivo que contém a imagem do `hsmroot`. Esta partição tem capacidade de 45MB e posteriormente será referenciada como CF.

A última partição física também é montada no sistema de arquivos na inicialização do `hsmroot`. Esta partição tem a única função de armazenar o log das

⁴Uma utilização de Engine OpenSSL é descrita na seção 3.7.2.3.

operações realizadas pelo HSM. Esta partição tem capacidade de 55MB e posteriormente será referenciada como partição de logs.

Ao todo o HSM tem 120MB de armazenamento persistente de dados, e 25MB de dados armazenados e executados da memória RAM.

3.1.3 Unidade de Gerência

O HSM é separado fisicamente em duas unidades, a primeira delas conhecida como Unidade de Gerência, ou apenas UG. A UG contém os componentes de hardware essenciais de qualquer computador, sendo os principais:

- Placa mãe ALIX, modelo alix3d2
- Processador AMD Geode 500MHz
- Memória 256MB DDR DRAM
- Compact Flash com capacidade de 1GB

Na CF (Compact Flash) da UG estão contidas as partições de dados descritas na seção 3.1.2.

A UG é protegida por vários sensores que são controlados pela US. Os sensores mais importantes são:

- Luminosidade: disparado caso o perímetro protetor da UG seja violado e um feixe de luz seja detectado.
- Estresse mecânico: disparado ao chocar o equipamento com algo ou derrubá-lo no chão.
- Temperatura: disparado ao esquentar ou resfriar o HSM de forma excessiva.
- Tensão: disparado caso ocorra a elevação da tensão de entrada.

3.1.4 Unidade de Segurança

A Unidade de Segurança, ou apenas US, está fisicamente separada da UG. A US é responsável por manter uma chave criptográfica que pode ser empregada em mecanismos de proteção do HSM contra técnicas de engenharia reversa e outras formas de ataque ao HSM. A US tem um mecanismo de controle do relógio mais preciso que a UG, pois ela dispõe de um relógio de alta estabilidade.

A funcionalidade criptográfica mais importante da US é a sua participação na geração de números aleatórios pelo HSM, pois a semente usada no algoritmo é gerada na US, em hardware. O gerador de números aleatórios do ASI-HSM não é pseudo-aleatório, pois em teoria o fenômeno utilizado para gerar uma semente em hardware não pode ser previsto.

Outra função da US é a de controlar e verificar os sensores que detectam alterações na UG. Os principais sensores estão descritos na seção 3.1.3. Caso algum destes sensores seja violado, a US emite um aviso informando que foi detectado um ataque ao HSM.

3.2 Grupos de Gerenciamento

Para a execução das funções do HSM é necessária a autenticação dos indivíduos responsáveis por aquela função, ou seja, aqueles que tem permissão para executá-la.

O ASI-HSM suporta a criação de grupos que podem ter de 1 a M membros, sendo o $M \geq 1$, para os casos onde há a necessidade da autorização de várias pessoas para a execução da tarefa o M será > 1 . A autenticação de um grupo é melhor explicada na seção 3.3.

No ASI-HSM existem três tipos de grupos de gerência, e os grupos de gerência fazem parte de um perfil de gerência. Esta nomenclatura ficará mais clara na medida que a leitura é realizada. Não é possível afirmar que um perfil no ASI-HSM é mais importante que o outro, pois suas funções se complementam para o funciona-

mento harmonioso do equipamento.

3.2.1 Administração

O perfil de administração no ASI-HSM só possui um grupo, ou seja, não é possível haver mais de um grupo ativo administrando o HSM simultaneamente, mas existe a possibilidade de se alterar o grupo existente, excluindo o grupo antigo e criando um grupo novo. Este é o perfil responsável por criar todos os outros grupos do HSM. Além disso suas principais funções no HSM são:

- Apagar configurações
- Atualizar firmware
- Desligar
- Alterar data/hora
- Gerar/Recuperar backup
- Gerar par de chaves assimétricas

O grupo de administradores é o primeiro grupo a ser criado no ASI-HSM, e pode ser trocado, mas nunca excluído.

3.2.2 Auditoria

O perfil de auditoria no ASI-HSM tem a responsabilidade de verificar o bom andamento das operações do módulo. É possível que um HSM possua mais de um grupo de auditores e é necessário que exista pelo menos um grupo. Suas principais funções no HSM são:

- Exportar logs
- Bloqueio do equipamento

- Recuperar backup

Após a criação de um grupo de auditores, ele não pode ser excluído.

3.2.3 Operação

O perfil de operação no ASI-HSM é o responsável por gerenciar o uso de chaves criptográficas. A criação de chaves criptográficas é função do perfil de administração, mas a decisão de quando utilizar as chaves e quantas vezes elas serão utilizadas fica a cargo do grupo de operadores responsável pela chave. Suas principais funções no HSM são:

- Carregar chave para uso
- Definir políticas de utilização da chave
 - Tempo de uso
 - Número de usos

Após a criação de um grupo de operadores, ele não pode ser excluído.

3.2.4 Funções Comuns a Todos os Perfis

Existem várias operações no ASI-HSM que não necessitam de autenticação por se tratarem de operações onde não existe o tráfego de informações sigilosas, operações como verificar a versão do software do ASI-HSM, mostrar seu estado atual, realizar auto-testes, listar grupos e membros de grupos de gerência, entre outras.

As duas funções mais importantes que podem ser executadas sem autenticação são o descarregamento de uma chave carregada e a configuração do ASI-HSM. O carregamento de uma chave privada para uso só pode ser realizado pelo grupo de operadores responsável por aquela chave, mas o descarregamento pode ser executado sem autenticação. A configuração do ASI-HSM é uma tarefa de inicialização do equipamento para uso e ela ocorre antes mesmo da criação do grupo de operadores, ou seja,

não há meios de se executar uma autenticação visto que não existe nenhum grupo criado.

3.3 Autenticação

No ASI-HSM existem três tipos de grupos que necessitam de autenticação, como foi descrito na seção 3.2. A autenticação de um grupo de gerência deve ser realizada toda vez que é uma função que necessita de autenticação é invocada.

O tamanho do grupo de gerência é definido no momento de sua criação. O grupo deve ter um M , que é número máximo de participantes, e um N , que é o número de participantes necessários para a autenticação, tal que $1 \leq N \leq M$.

A operação é realizada após a autenticação de N membros do grupo de gerência. Esse método de autenticação é possível utilizando o método do segredo compartilhado, explicado na seção 2.1.4.

3.4 Chaves Gerenciadas

As chaves gerenciadas pelo ASI-HSM possuem um grupo de operadores que mantém a sua custódia, ou seja, são responsáveis por definir quando a sua chave será utilizada e quantas vezes a chave pode ser utilizada.

Para que uma chave privada possa ser utilizada (e.g. assinatura de um arquivo), ela deve ser carregada em memória pelo grupo de operadores responsável por ela. No momento da operação, o grupo de operadores define por quanto tempo a chave permanecerá carregada em memória, e quantas vezes ela poderá ser utilizada. Em seguida é possível utilizar a chave, se fazendo uso da Engine OpenSSL do ASI-HSM, descrita na seção 3.7.2.3.

A exportação da chave pública não precisa do consentimento de nenhum grupo de gerência, visto que a chave pública não é sigilosa, assim como a operação de descarregamento da chave privada, pois isso não compromete a sua segurança.

3.5 Backup

A função de backup do ASI-HSM é extremamente importante, pois é ela que garante a continuidade das chaves privadas armazenadas, mesmo na eventual falha do equipamento e a destruição das mesmas.

O backup é composto por um pacote de arquivos que é cifrado com a chave pública de outro HSM. Isso é necessário para garantir que o pacote de backup gerado só possa ser restaurado no HSM que mantém a chave privada desse par. Esse procedimento é chamado backup direcionado.

Este pacote de arquivos que é gerado, contém as informações referentes às configurações do HSM, grupos de gerência, chaves gerenciadas, entre outros dados. Para gerar um pacote de backup é necessária a autenticação do grupo de administradores.

Na restauração de um pacote de backup, esta restauração só pode ocorrer no HSM para onde o backup foi direcionado, visto que o pacote está cifrado com sua chave pública. A restauração necessita da autenticação do grupo de administradores e de um grupo de auditores.

3.6 Update de Firmware

O update de firmware é uma operação que necessita da autenticação do grupo de administradores. O pacote de firmware é um arquivo no formato PKCS#7 assinado pelo fabricante do ASI-HSM, e somente um pacote com essa assinatura pode ser utilizado no update, pois qualquer outro pacote é rejeitado pelo HSM.

No update são atualizados o kernel do SO e o *hsmroot*.

3.7 Interfaces

Para a comunicação externa com o ASI-HSM e a sua alimentação elétrica, existem quatro interfaces físicas e três interfaces lógicas.

3.7.1 Interfaces Físicas

As interfaces físicas do ASI-HSM são:

- Alimentação elétrica: entrada J4 para tensão de 12V.
- Interface de rede RJ-45: utilizado para transferência de dados entre o HSM e o computador hospedeiro.
- Leitora de Smart Card: entrada para a leitura dos Smart Cards, usados na autenticação dos usuários.
- Porta USB: pode ser utilizada para a escrita de dados em um token USB, ou para o uso de uma leitora de Smart Cards externa.

3.7.2 Interfaces Lógicas

As interfaces lógicas para uso, configuração e administração do ASI-HSM são três, a interface gráfica Java, o cliente texto e a Engine OpenSSL. As duas primeiras são usadas para configuração e administração do módulo, a Engine OpenSSL é usada para utilizar os serviços providos pelo ASI-HSM.

As interfaces de administração do módulo se comunicam com o HSM utilizando protocolo de comunicação segura TLS/SSL, descrito na seção 2.3.

3.7.2.1 Interface Gráfica Java

A interface gráfica Java foi implementada usando a linguagem Java, como o próprio nome já indica. A interface pode ser utilizada para executar as funções de administração, auditoria e operação do HSM, operações descritas na seção 3.2. A escolha da linguagem Java para a implementação se deu pela portabilidade de uso da aplicação, que pode ser executada tanto em Linux como em Windows, ou em qualquer sistema operacional com um servidor X (interface gráfica) e a máquina virtual Java versão 1.6 ou superior.

3.7.2.2 Cliente Texto

A interface cliente texto é uma aplicação em linha de comando UNIX (shell), que é equivalente à interface gráfica Java em termos de funcionalidades.

3.7.2.3 Engine OpenSSL

Para se fazer uso dos serviços providos pelo ASI-HSM utiliza-se a Engine OpenSSL. Uma engine OpenSSL pode ser carregada por uma aplicação que faz uso da biblioteca OpenSSL, ou pode ser carregada em linha de comando. No momento da chamada de função, a engine é utilizada para se comunicar com o HSM, executando a função criptográfica requisitada. A função irá falhar caso ela requisite a utilização de uma chave privada que não está carregada para uso.

As funções OpenSSL mais importantes providas pelo ASI-HSM são:

- `openhsm_engine_private_decrypt`: decifragem de dados.
- `openhsm_engine_private_encrypt`: cifragem de dados.
- `openhsm_load_private_key`: carrega uma chave privada.
- `openhsm_load_public_key`: carrega uma chave pública.

Capítulo 4

Homologação na ICP-Brasil

Este capítulo demonstra como é o processo de homologação de um Módulo de Segurança Criptográfica na ICP-Brasil, quais as etapas envolvidas e os procedimentos que devem ser executados pelos interessados na homologação.

A instituição que iniciou o processo de homologação do ASI-HSM é a RNP, no contexto deste trabalho. A Parte Interessada, ou simplesmente PI, é a maneira como o ITI se refere à RNP durante grande parte do processo.

4.1 Órgão Homologadores

A homologação de um equipamento é realizada por um órgão que realiza ensaios no mesmo, verificando se ele está de acordo com as suas normas e padrões. A homologação de equipamentos não se dá apenas em módulos de segurança criptográfica, outros setores que podem ser citados são o automotivo, semicondutores, comunicações e construção. [Nat 09b]

4.1.1 NIST

O NIST (National Institute of Standards and Technology) é um órgão americano que estabelece normas, medidas e padrões para várias áreas tecnológicas. Neste trabalho serão feitas várias referências à norma FIPS 140-2.

A norma FIPS 140-2 contém a descrição dos requisitos que um módulo de segurança criptográfica deve atender para estar de acordo com os padrões do NIST, e por consequência ser homologado caso seja submetido a esse processo. Quem realiza os ensaios e verifica a conformidade de um HSM com a FIPS 140-2 é o CMVP (Cryptographic Module Validation Program), que é um programa criado em 1995 pelo NIST em conjunto com o CSEC (Communications Security Establishment Canada). [Nat 09c][Com 09]

Para que um HSM possa ser utilizado em agências federais dos Estados Unidos da América ou Canadá, ele precisa ser homologado pelo NIST.

Para o NIST, informação valiosa ou dados sensíveis protegidos por um HSM que não está de acordo com a norma FIPS 140-2, são considerados dados desprotegidos. Essa preocupação demonstra a importância do processo de homologação.

4.1.2 ITI

Assim como o NIST estabelece normas para órgãos americanos, o ITI (Instituto de Tecnologia da Informação) estabelece normas para garantir a segurança da informação no âmbito da ICP-Brasil. [Ins 09b][Ins 09a]

O ITI é uma autarquia da Presidência da República e é responsável por manter a ICP-Brasil, que é a Infra-Estruturas de Chaves Públicas Brasileira.

Assim como o NIST e o CSEC, o ITI compõe normas e padrões para a homologação de vários tipos de equipamentos como smart cards, leitoras de smart cards, bibliotecas criptográficas e o nosso objeto de estudo, módulos de segurança criptográfica. Para cada equipamento passível de ser homologado, existe um documento chamado MCT (Manual de Condutas Técnicas), que é um documento contendo os requisitos necessários para que o equipamento esteja em conformidade com os padrões do ITI. [Inf 09c]

Para a homologação de um módulo de segurança criptográfica, o MCT 7 é o documento que contém os requisitos, e este será o documento abordado neste trabalho. A abordagem do MCT 7 será realizada no capítulo 5.

A entidade responsável pela realização dos ensaios é chamada LEA (Laboratório de Ensaios e Análise), que foi o responsável pela avaliação do ASI-HSM, verificando se todos os requisitos do MCT 7 foram cumpridos.

4.2 Níveis de homologação

Existem vários níveis possíveis de serem escolhidos para homologar um equipamento na ICP-Brasil. Estes níveis definem o grau de confiabilidade que o ITI pôde atribuir ao equipamento homologado. Quanto menor o nível de homologação, menos materiais a PI deve entregar ao ITI para realizar a análise, assim a transparência do equipamento fica prejudicada no processo.

Existem dois tipos de níveis de homologação, conhecidos como nível de segurança de homologação e nível de segurança física.

4.2.1 Níveis de segurança de homologação

Existem três níveis de segurança de homologação (ou simplesmente NSH) no ITI.

4.2.1.1 NSH 1

O NSH 1 é um nível bastante simples, pois só é necessário o depósito do HSM objeto de homologação e de manual contendo instruções de uso.

Os testes ocorrem em um ambiente onde as ameaças de segurança são controladas, ou seja, os testes de invasão do HSM e segurança das chaves não é feito com menor rigor.

Basicamente são testes de funcionalidades, verificando se o HSM cumpre os requisitos que o caracterizam como um equipamento que provê serviços criptográficos e de gestão do ciclo de vida de chaves criptográficas.

4.2.1.2 NSH 2

No NSH 2 a PI deve depositar partes do código-fonte e informações sobre o projeto, pois nesta etapa as ameaças de segurança já não são controladas, ou seja, o HSM deve manter a segurança das chaves em um ambiente onde a ameaça à segurança do equipamento é relevante. Neste nível é necessária a confiança nas operações do equipamento.

4.2.1.3 NSH 3

Este é o maior nível de segurança de homologação na ICP-Brasil, e é o nível ao qual o ASI-HSM foi submetido. O NSH 3 deve atender a tudo o que o NSH 2 requer, mas com um rigor muito maior. O HSM deve manter a segurança das chaves a um nível crítico, ou seja, em um ambiente hostil de armazenamento, que é caracterizado por um ambiente com pouco monitoramento e controle de acesso fraco.

Devem ser fornecidas informações de projeto detalhadas e completas, e todo o código-fonte do HSM. Neste nível também é necessária a comprovação de utilização de práticas seguras no desenvolvimento e fabricação do HSM, para que seja comprovado que o HSM provê segurança das informações desde o momento de sua fabricação.

4.2.2 Níveis de segurança de física

Existem dois níveis de segurança física (ou simplesmente NSF) no ITI.

4.2.2.1 NSF 1

O NSF 1 é um nível de segurança física que garante que será possível identificar que o HSM foi violado fisicamente, caso isso ocorra. Vale notar que essa identificação é uma simples evidenciação de que houve a violação, não é necessário que o HSM responda ao ataque.

4.2.2.2 NSF 2

Este é o maior nível de segurança física na ICP-Brasil, e é o nível ao qual o ASI-HSM foi submetido. No NSH 3 o HSM além de evidenciar que ocorreu uma violação física, deve responder ao ataque. Caso ocorra um ataque ao ASI-HSM, onde terceiros tentem obter acesso às chaves armazenadas, a forma adotada de impedir esse acesso é a destruição das chaves. É requisito da homologação que a destruição aconteça na ocorrência de um ataque.

4.3 Processo de Homologação

O processo de homologação será apresentado em três etapas para facilitar o seu entendimento como um todo. O fluxograma contendo as etapas pode ser encontrado no apêndice A.

Os documentos que serão explicados abaixo podem ser encontrados no website do ITI, na página referente a homologação.

4.3.1 Entrega de documentação técnica e jurídica

A homologação de um HSM passa por várias etapas que não são apenas de análise e ensaios do equipamento. A primeira etapa é um processo burocrático, estudo e entrega de documentos jurídicos e troca de contatos.

4.3.1.1 Agendamento de atendimento

A PI deve entrar em contato com o ITI solicitando agendamento para a entrega da documentação referente ao equipamento a ser homologado. O ITI selecionará local, data, horário e pessoa de contato para que a PI possa apresentar os documentos.

4.3.1.2 Habilitação jurídica

Na habilitação jurídica a um representante da PI deve entregar os seguintes documentos:

- Formulário de requerimento de homologação: documento padrão com informações básicas, como endereço, razão social da PI, sistemas ou equipamentos a serem homologados, entre outros.
- Prova de inscrição do CNPJ.
- Termo de propriedade intelectual: documento que comprova que a PI detém a propriedade intelectual dos equipamentos a serem depositados para homologação.
- Termo de sigilo: um contrato assinado entre o ITI e a PI para que nenhuma das partes faça a divulgação de material que possa prejudicar a outra.

Caso os documentos estejam corretos, é entregue para o representante da PI um protocolo de habilitação jurídica, que contém detalhes de local, data e horário para o depósito do equipamento.

4.3.1.3 Depósito dos sistemas e equipamentos

A PI faz o depósito do equipamento submetido à homologação e seus acessórios, caso houverem, conforme instruções contidas no protocolo de habilitação jurídica recebido na etapa anterior.

Os artefatos depositados serão utilizados posteriormente para a realização dos ensaios.

No caso do ASI-HSM, foi realizado o depósito de:

- Um HSM operacional
- Um HSM não operacional
- Smart card

- Leitora de smart card
- Manual do usuário ASI-HSM
- Todo o código-fonte dos componentes de software
- Todo o código-fonte dos componentes de hardware, caso seja aplicável
- Documento de requisitos

O documento de requisitos, que é um dos artefatos depositados, é um documento contendo a descrição das informações de funcionamento e de projeto do HSM. Esse documento é totalmente produzido pela PI e comprova que o HSM atende aos requisitos do MCT 7.

4.3.1.4 Análise quantitativa

Esta é uma análise bastante rápida, onde o ITI irá verificar se o material que foi depositado é o mesmo material que foi declarado para depósito na etapa de habilitação jurídica.

4.3.1.5 Análise qualitativa

Neste momento o ITI tem em mãos o ASI-HSM, o código-fonte de todos os seus componentes, o manual do usuário e o documento de requisitos. O documento de requisitos contém a descrição do funcionamento do ASI-HSM e a explicação de como o ASI-HSM atende aos requisitos do MCT 7.

Esse material é necessário para que o ITI tenha condições de analisar o equipamento e verificar se a documentação técnica atende aos requisitos do MCT 7.

Caso o LEA verifique que o documento de requisitos está incompleto, ou que algum requisito não está em conformidade, é emitido um parecer pelo ITI contendo detalhes que na maioria das vezes auxiliam a PI a entender o que está faltando. No contexto deste trabalho, vários problemas apareceram que ocasionaram à não conformidade do ASI-HSM com alguns requisitos do MCT 7, entre elas:

- Significado do requisito: muitas vezes não entendíamos exatamente o que o requisito imposto realmente queria dizer, por isso o documento de requisitos era entregue com uma descrição errada ou incompleta. Uma descrição correta resolvia o problema.
- Descrição pouco didática: a nossa descrição de como funcionava algum procedimento no ASI-HSM, não estava escrita de forma clara, o que tornava difícil ou impossível o entendimento pelo LEA.
- HSM não suportava o requisito: algumas funções que o ASI-HSM precisava suportar para ser homologado, simplesmente não existiam, e foi necessária a implementação dessas funções para prosseguir com o processo de homologação. As funções implementadas estão descritas no capítulo 6.

Caso o LEA entenda que a descrição de todos os requisitos está de acordo, o ITI envia cópia do relatório da análise qualitativa para a PI e o processo prossegue para a próxima etapa.

4.3.1.6 Análise de conformidade

Com o documento de requisitos e o equipamento a ser homologado em mãos, o LEA pode iniciar os ensaios de conformidade. Caso o LEA sinta a falta de algum componente para que a realização dos ensaios seja realizada, o ITI encaminha um parecer que é encaminhado para a PI, requisitando o equipamento faltante. A PI deve depositar os equipamentos solicitados para que o processo continue.

4.3.1.7 Homologação

Durante todo o processo de homologação, o LEA realiza as análises quantitativa, qualitativa e de conformidade. O LEA é um laboratório credenciado pelo ITI para realizar ensaios de homologação, se o LEA afirmar que o HSM passou com sucesso por todas as análises, ou seja, que está em conformidade com os requisitos do MCT 7, o equipamento é homologado e recebe o selo da ICP-Brasil.

Caso o HSM não consiga comprovar a conformidade em qualquer uma das etapas, ele não será homologado na ICP-Brasil. Se a PI mostrar interesse em tentar a homologação mais uma vez, ela deve reiniciar o processo.

Capítulo 5

Requisitos do MCT 7

Este capítulo explica o que significa uma homologação de HSM na ICP-Brasil, e quais os requisitos necessários para que a homologação seja concluída.

A série de requisitos que um HSM deve atender para estar de acordo com o MCT 7 pode ser dividida em vários tipos diferentes, que vão desde requisitos descritivos do equipamento, até requisitos que se referem a funcionalidades e documentação.

5.1 Descrição

Os requisitos descritivos são importantes para que o LEA possa entender o contexto do HSM antes de começar os ensaios, e até mesmo ter um material de referência caso ocorra alguma dúvida durante os ensaios. Foi bastante comum fazer uso de referência a esses requisitos durante a explicação de funcionalidades complexas do equipamento, que necessitavam do conhecimento de outras partes do módulo.

Alguns requisitos requerem a descrição de:

- Visão geral do software, hardware e firmware;
- Configuração física;
- Portas físicas, interfaces lógicas e caminhos de dados;
- Indicadores de estados físicos e lógicos;

- Características elétricas, lógicas e físicas (i.e. voltagem e dimensões);
- Funções e operações criptográficas;
- Esquemas de hardware;
- Controladores de hardware utilizados;
- Ambiente Operacional;
- Softwares e bibliotecas utilizadas;
- Armazenamento de dados sensíveis (i.e. chaves criptográficas);
- Mitigação de ataques.

Requisito

REQUISITO III.1.8: A parte interessada deve fornecer documentação específica que liste todas as funções de segurança e operações criptográficas que são empregadas pelo módulo, assim como especificar todos os modos de operação suportados, tanto os aprovados e os não-aprovados por um órgão homologador como o CMVP para FIPS 140.

Resolução

Neste requisito foi descrita a utilização dos algoritmos:

- Gerador de números aleatórios: OpenSSL FIPS e semente aleatória gerada em hardware (detalhes na seção 3.1.4)
- Geração de chaves assimétricas: RSA
- Assinatura digital: RSA
- Compartilhamento de segredo: Shamir

- HASH: SHA-1
- Certificados digitais¹: SHA1 com RSA
- Chaves simétricas: AES nos modos ECB e CBC com tamanhos de chaves suportados 128, 192 e 256 bits. 3DES nos modos ECB e CFB com chaves de tamanho 168 bits.

5.2 Proteção das chaves

Proteger as chaves criptográficas armazenadas no módulo significa impedir que qualquer indivíduo não autorizado tenha acesso ou possa utilizar essas chaves. A proteção deve ser física e lógica.

5.2.1 Proteção física

O HSM deve possuir mecanismos de proteção física de seus componentes, e em especial das chaves criptográficas.

Requisito

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

Resolução

Dentre os mecanismos de proteção física do ASI-HSM, podemos citar:

- Evidenciação de abertura: lacres produzidos com papel extra-fino envolvem as extremidades do gabinete interno do HSM, sendo assim muito fácil identificar se houve a tentativa de abertura do gabinete.

¹Certificados digitais X.509 utilizados para administração interna do ASI-HSM

- Perfuração: sensores que cobrem toda a sua superfície, disparando a qualquer sinal de interrupção.
- Ataques EMI (Electromagnetic Interference): malha de cobre que impede a entrada ou saída de emissões eletromagnéticas.
- Luminosidade: sensores que evidenciam a entrada de luz no gabinete interno.
- Temperatura: sensores que disparam no aquecimento ou resfriamento excessivo do HSM.
- Tensão: medidores de tensão, disparados quando a tensão atinge valores fora do padrão.

Estes métodos de proteção dificultam a ação do adversário de modificar ou substituir as chaves armazenadas em disco. A única maneira de modificar as chaves com sucesso seria burlar todos os sensores, o que é extremamente difícil.

É requisitado que o HSM destrua todo o conteúdo crítico (chaves, dados de usuários) assim que um ataque físico é detectado.

5.2.2 Proteção lógica: uso indevido

Requisito

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

Resolução

A autenticação é necessária para qualquer função que necessita de privilégios de algum grupo no ASI-HSM. Detalhes sobre autenticação podem ser encontrados na seção 3.3.

Somente usuários autorizados podem fazer uso das chaves criptográficas. Para garantir essa proteção, cada chave é cifrada pelo grupo de operadores que detêm a

custódia da mesma e dessa maneira ela é armazenada em disco. Com isso há a garantia de que as chaves não serão utilizadas indevidamente.

5.2.3 Proteção lógica: algoritmos aprovados FIPS

Para que um conteúdo cifrado no HSM seja considerado seguro, ele deve estar cifrado com um algoritmo aprovado por alguma norma FIPS vigente. O mesmo é válido para algoritmos de assinatura digital (criptografia assimétrica), algoritmos de HASH e segredo compartilhado.

Também se faz necessário que o algoritmo RNG (random number generator) seja aprovado FIPS.

Um requisito de exemplo é o mesmo descrito na seção 5.1.

Atualmente o ASI-HSM suporta o RSA para assinatura digital, SHA-1 para HASH, AES e 3DES para criptografia simétrica e Shamir para o método do segredo compartilhado. Todos estes algoritmos são utilizados a partir da biblioteca criptográfica OpenSSL versão FIPS, que é uma biblioteca criptográfica aprovada pela norma FIPS. O algoritmo RNG usado também é o implementado pelo OpenSSL FIPS².

5.2.4 Proteção lógica: exportação de chaves

Requisitos

REQUISITO III.7.21: Chaves secretas e privadas importadas utilizando métodos manuais devem entrar no módulo criptográfico ou sair do módulo criptográfico:

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

²O OpenSSL FIPS pode ser encontrado no website do OpenSSL, assim como instruções de instalação e manual do usuário

REQUISITO III.7.25: Chaves assimétricas públicas devem ser exportáveis do módulo criptográfico.

OBSERVAÇÃO: Uma chave pública pode ser importada ou exportada do módulo criptográfico em texto claro.

Resolução

A exportação de chaves criptográficas é uma operação extremamente sensível. No ASI-HSM a exportação de chaves públicas não requer qualquer tipo de autenticação. A exportação de chaves privadas não é suportada pelo ASI-HSM, exceto no procedimento de backup.

No procedimento de backup todos os dados de configuração e chaves do HSM são exportados cifrados com a chave pública do HSM destino, como está descrito na seção 3.5. Esses dados também são cifrados com a chave do perfil de administração, para que os usuários com a função de administrador saibam que um backup foi restaurado, visto que a autenticação dos mesmos é necessária para decifrar os dados. Mais importante que isso, cifrar o conteúdo com a chave do perfil de administração garante a proteção dos dados do HSM.

5.2.5 Proteção lógica: sobrescrita com zeros

Requisito

REQUISITO III.7.30: O módulo deve prover métodos para sobrescrever com zeros binários os valores de todas as chaves simétricas, chaves assimétricas privadas e PCSs.

Resolução

Quando uma chave privada é liberada para uso, ela é armazenada em texto claro na memória volátil, conforme descrito na seção 3.4.

Assim que a chave não é mais necessária, por expiração do tempo de uso

ou porque os usos permitidos já se esgotaram, o HSM precisa removê-la da memória. O processo de remover a chave da memória é chamado “zeramento” (ou zeramento binário na nomenclatura do MCT 7), onde o algoritmo responsável sobrescreve o espaço de memória ocupado pela chave com zeros³, assim a chave é destruída.

5.3 Documentação

Requisitos

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

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

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

Resolução

O MCT 7 preocupa-se também com os usuários do HSM, no sentido de que eles devem entender como o equipamento funciona. Para realizar essa comunicação entre o fabricante e o usuário, foi desenvolvido o Manual do ASI-HSM.

O Manual do ASI-HSM é um documento público desenvolvido pelo Lab-SEC e pela Kryptus, descrevendo de forma detalhada as operações que podem ser realizadas no ASI-HSM. Algumas informações que podem ser encontradas no manual a respeito do equipamento são:

- Instalação;
- Configuração;

³Não é necessário preencher o espaço com zeros, preenchê-lo com bits aleatórios é suficiente.

- Criação de grupos;
- Criação de chaves;
- Execução de auto-testes;
- Atualização de firmware;
- Geração e recuperação de backup;
- Estados do HSM;
- Modo de segurança;
- Práticas seguras de uso.

O Manual do ASI-HSM é hospedado na página do projeto OpenHSMd, em: <https://projetos.labsec.ufsc.br/openshsmd>.

5.4 Usabilidade

É importante que os usuários saibam o que está ocorrendo com o HSM em todos os momentos, visto que os dados que ele carrega são sensíveis e podem ser muito importantes dependendo do contexto (i.e. AC-Raiz Brasileira). [Ins 09a]

Um dos requisitos para a homologação é que se apresente um diagrama de estados do HSM, contendo todos os estados operacionais, estados de erro e transições de estado resultantes de eventos de entrada e saída do módulo.

A partir dos estados mapeados, o HSM deve informar ao usuário em qual estado o equipamento se encontra, quando lhe for requisitado.

Para o HSM em estado de erro, é necessário que ele tenha um Modo de Segurança, onde suas funções são limitadas até que ele seja colocado em estado operacional.

A confecção do diagrama de estados e o Modo de Segurança foram inovações no ASI-HSM, cujas descrições podem ser encontradas na seção 6.3.

5.5 Interoperabilidade

Requisito

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

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

Resolução

O usuário de um HSM deve ser capaz de invocar os requisitos funcionais do equipamento. O ASI-HSM possui duas interfaces de administração remota que são a Interface Gráfica Java e o Cliente Texto, descritas na seção 3.7.2. Com as duas interfaces é possível executar as funções do HSM em ambiente Linux kernel 2.4 ou superior e Windows 2000 ou superior, atendendo ao requisito.

Para fazer uso do serviço provido pelo ASI-HSM, que é o serviço de assinatura digital RSA, foi implementada uma Engine OpenSSL, descrita em detalhes na seção 3.7.2.3.

5.6 Funcionalidades

Existem requisitos que se referem a operações comuns de um HSM, que o caracterizam como um equipamento desse tipo.

5.6.1 Operação

Requisito

REQUISITO III.3.3: O módulo criptográfico deve suportar, no mínimo, os seguintes “papéis autorizados”:

- Oficial de Segurança (SO)
- Usuário
- Papel de Manutenção

OBSERVAÇÃO: Caso o MSC não suporte um papel específico de manutenção, as operações de manutenção serão feitas pelo oficial de segurança (SO).

Resolução

Os requisitos referentes a operações do módulo basicamente se referem às funções descritas nas seções 3.2 e 3.3. É necessário identificar os tipos de usuários seguindo a classificação do MCT 7 (herdada da FIPS 140-2) descrita acima.

No caso do ASI-HSM foi necessário explicar o mecanismo de autenticação empregado pelo módulo e informar quais são os grupos de gerenciamento semelhantes aos definidos pelo MCT 7.

Os usuários “Oficial de Segurança” e “Manutenção” podem ser caracterizados pelo perfil de Administração, pois ele é o responsável por executar operações de manutenção e pela geração de chaves. O usuário “Usuário” é semelhante ao perfil de Operação, responsável por carregar as chaves para uso. O perfil de auditoria acaba executando uma operação do usuário “Manutenção”, que é a exportação e exclusão de logs.

5.6.2 Auto-testes

Um HSM deve possuir funções que realizem testes para constatar o bom funcionamento do módulo, chamadas de auto-testes.

Uma categoria dos auto-testes são os testes de energização. Os auto-testes de energização são aqueles executados quando o HSM é ligado ou reiniciado.

Outra categoria são os auto-testes realizados quando um componente de software ou firmware é importado para o HSM. O HSM deve prover meios de autenticar o componente importado. Caso a autenticação falhe, o componente não deve ser importado.

A última categoria são os auto-testes condicionais de algoritmos utilizados pelo HSM. Os auto-testes são condicionais, pois eles devem ser executados durante a inicialização e a qualquer momento que o usuário requisitar.

Caso o resultado de um auto-teste seja uma falha, o usuário deve ser informado dessa falha. Quando o HSM está em estado de erro, qualquer operação criptográfica deve ser impedida de ser realizada, e nenhum dado pode sair do HSM.

A execução de auto-testes foi um aprimoramento do ASI-HSM, e sua descrição está na seção 6.2.

Capítulo 6

Implementação

Este capítulo é referente à implementação necessária para que o ASI-HSM entrasse em conformidade com os requisitos do MCT 7.

6.1 Modo de Segurança

No ASI-HSM não existia nenhuma solução para um estado de erro, para isso foi criado o Modo de Segurança. O ASI-HSM entra em modo de segurança sempre que um erro for detectado na inicialização ou nos auto-testes condicionais.

Quando o modo de segurança é ativado, o usuário é informado. Mais detalhes podem ser encontrados na seção 6.3.

6.2 Auto-Testes

A implementação dos auto-testes foi um dos fatores que aumentou em muito a robustez do ASI-HSM, mas também foi uma das funcionalidades mais complicadas de se implementar, visto que é bastante complexa e extensa.

Requisito

REQUISITO III.9.5: A documentação do módulo criptográfico deve especificar os seguintes itens:

- Os auto-testes realizados pelo módulo;
- O estado de erro que o módulo criptográfico pode entrar quando um auto-teste falha;
- 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).

Resolução

Este requisito é bastante genérico, pois pede a descrição de todos os auto-testes do módulo. A explicação dos auto-testes implementados estão nesta seção com a adição de outros requisitos necessários, e a descrição dos estados do ASI-HSM estão na seção 6.3.

6.2.1 OpenSSL FIPS

Requisito

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

REQUISITO III.9.8: A documentação deve listar todos os testes de funções criptográficas do tipo “resposta conhecida”.

Resolução

Os auto-testes OpenSSL FIPS se referem aos auto-testes condicionais de algoritmos do HSM. O OpenSSL FIPS é uma versão da biblioteca criptográfica OpenSSL

que foi submetida ao processo de homologação na norma FIPS 140-2.

O OpenSSL FIPS oferece uma função que coloca o HSM no que é chamado de modo FIPS. Assim que a aplicação entra em modo FIPS, só é possível utilizar funções criptográficas aprovadas FIPS, como RSA e SHA-1, não sendo possível utilizar funções não-aprovadas FIPS, como MD5 e IDEA.

No ASI-HSM os auto-testes são realizados no momento da inicialização do software de gerência, o OpenHSMd, pois no momento da inicialização é ativado o modo FIPS, e na rotina de ativação do modo FIPS é realizado o auto-teste das funções criptográficas. Caso algum auto-teste falhe, o modo FIPS não é ativado e o HSM entra em modo de segurança.

Durante o funcionamento normal é possível invocar a execução do auto-teste OpenSSL FIPS. Caso o usuário use a função, é mostrado para ele o resultado detalhado dos testes, assim ele saberá exatamente qual algoritmo falhou, se for o caso.

6.2.2 Unidade de Segurança

A US (Unidade de Segurança) (descrita na seção 3.1.4) é um componente extremamente importante do ASI-HSM, pois é ela que fornece a semente utilizada no algoritmo de geração de números aleatórios. Por ser um componente importante, é necessário verificar o bom funcionamento da US.

O auto-teste é realizado na inicialização do OpenHSMd, e também sob demanda, ou seja, o usuário pode invocá-lo por uma das interfaces de administração remota.

6.2.3 Integridade do Firmware

Requisito

REQUISITO III.9.10: Um método de autenticação aprovado será utilizado para todos componentes de software e firmware validados quando os componentes forem carregados externamente para dentro do módulo criptográfico.

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

Resolução

As aplicações do ASI-HSM estão no *hsmroot*, descrito na seção 3.1.2, sendo assim todas as funções criptográficas e de gerência de chaves são executadas no *hsmroot*.

Verificar a integridade do firmware é uma tarefa fácil, visto que todo o conteúdo do *hsmroot* é condensado em um único arquivo que é posteriormente carregado na memória no formato de uma partição. A solução encontrada foi adicionar um arquivo à CF, chamado *hsmroot.signedhash*, que é um arquivo de texto assinado pelo fabricante, contendo o HASH SHA-1 do *hsmroot*.

A seqüência de passos para a checagem de integridade do *hsmroot* é executada logo antes de seu carregamento em memória, e segue os passos:

- Verifica se o *hsmroot.signedhash* foi assinado pelo fabricante;
- Salva o conteúdo do arquivo *hsmroot.signedhash* na variável `hsmroot_hash`;
- Calcula o HASH SHA-1 do *hsmroot* e salva o resultado na variável `hsmroot_calculated_hash`;
- Verifica se `hsmroot_hash` e `hsmroot_calculated_hash` são iguais.

Se os valores forem iguais, significa que o *hsmroot* está íntegro, em caso contrário significa que não está íntegro e o ASI-HSM não inicia, pois a segurança dos dados contidos no módulo não pode ser garantida.

6.2.4 Energização

Requisito

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 críticas;
- Outros testes realizados na energização ou sob demanda.

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

Resolução

Um teste não foi necessário implementar, que é o teste de integridade das partições. Esse teste é realizado na rotina de inicialização do ASI-HSM, antes mesmo de carregar o *hsmroot* em memória. O teste é bastante simples e faz uso da aplicação *fsck*, que recebe como parâmetro a partição a ser analisada, corrigindo falhas na partição na medida do possível.

Os auto-testes de energização são realizados na seguinte ordem:

- Integridade das partições;
- Integridade do módulo;
- OpenSSL FIPS;
- Unidade de Segurança;

6.2.5 Importação de Firmware

Requisito

REQUISITO III.9.10: Um método de autenticação aprovado será utilizado para todos componentes de software e firmware validados quando os componentes forem carregados externamente para dentro do módulo criptográfico.

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

Resolução

Na importação de um firmware no HSM, é necessário que o módulo faça a sua autenticação e verificação, para que não sejam carregados softwares que não sejam aprovados pelo fabricante, e para que o usuário saiba se o que está sendo carregado é aquilo que ele quer que seja carregado.

No ASI-HSM o pacote de firmware é assinado pelo fabricante do equipamento. O ASI-HSM verifica se o pacote foi realmente assinado pelo fabricante, em caso positivo a operação continua, pois a autenticidade do pacote foi confirmada. Caso a autenticidade não possa ser comprovada, o pacote é descartado e a operação para.

Para garantir a integridade na operação, é calculado o HASH SHA-1 do pacote de firmware. O HASH é então mostrado para o usuário, que deve conferir se o HASH é o mesmo do arquivo que ele enviou para o HSM. Caso o usuário confirme, a operação continua, senão o pacote é descartado e a operação para.

6.3 Estados do Módulo

Requisito

REQUISITO III.4.1: O diagrama de transição de estados e/ou a tabela de transição de estados deve incluir:

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

Resolução

Para atender aos requisitos do MCT 7, foi criado um diagrama de estado finitos que define os estados do ASI-HSM. Foi necessário diferenciar o que são estados de erro e o que são estados de operação normal do módulo.

O diagrama de estados pode ser visualizado no apêndice B.

6.3.1 Estado Operacional

Quando nenhum erro é detectado no ASI-HSM, significa que ele está em Estado Operacional ou Modo Operacional. Em Modo Operacional todas as funções estão habilitadas para uso.

6.3.2 Estado de Erro

Quando um erro é detectado no ASI-HSM, significa que ele está em Estado de Erro ou Modo de Segurança. No Modo de Segurança as funções do ASI-HSM são bastante limitadas, pois nesse estado a segurança das operações não pode ser garantida.

Por esse mesmo motivo todas as chaves são descarregadas e não podem ser utilizadas até que se saia do Modo de Segurança.

Existem duas categorias de estados de erro, sendo a primeira delas o estado de erro recuperável. Um erro recuperável é aquele que pode ser sanado com a reinicialização (*reboot*) do HSM. Erros dessa categoria são o mal funcionamento da US ou o desligamento abrupto do equipamento.

A segunda categoria de estados de erro é o estado de erro crítico, ou estado de erro irre recuperável. Um erro irre recuperável é aquele que só pode ser sanado com o retorno do equipamento para o fabricante ou a sua destruição, no caso de conter dados muito importantes. Um erro irre recuperável pode ser causado por uma falha de hardware da US, detecção de um ataque, falha na verificação de integridade de firmware, falha em auto-teste OpenSSL FIPS.

Para tentar recuperar o ASI-HSM é possível executar a função “Modo Operacional” a partir de uma das interfaces de gestão remota. Se o HSM reiniciar em modo operacional, significa que se tratava de um erro recuperável, em caso contrário, o erro é crítico.

6.4 Segregação de Dados

É necessário garantir que a geração de chaves no HSM possa ser realizada com sucesso. Na estrutura de partições que era usada anteriormente no ASI-HSM, a partição que armazenava as chaves e logs era a mesma, o que poderia causar falta de espaço em disco para a geração de novas chaves, pois o log poderia crescer a ponto de ocupar todo o espaço.

Este problema foi amenizado com a reorganização da estrutura de partições, onde a partição de chaves (CF) foi separada da partição de logs. Uma descrição mais detalhada dessas partições pode ser encontrada na seção 3.1.2.

6.5 Nível Crítico do Espaço em Disco

Por questões de usabilidade, é interessante que o usuário do HSM saiba quando o espaço em disco atingiu um nível crítico. Para isso foi implementada uma verificação de espaço em disco no momento em que uma das interfaces de gestão remota se conecta ao ASI-HSM.

Caso o espaço em disco seja pequeno, é exibido um aviso na tela informando qual partição está em nível crítico. É considerado nível crítico para a partição de chaves quando o espaço em disco é menor que 3MB, que representa aproximadamente 18,75% do espaço total para armazenamento de chaves em um HSM que acaba de sair de fábrica. Para a partição de logs o nível crítico é quando o espaço em disco é menor que 5MB, que representa aproximadamente 9% do espaço total para armazenamento de logs.

Capítulo 7

Considerações Finais

A homologação do ASI-HSM na ICP-Brasil é um processo que ainda está em andamento, pois o HSM se encontra na fase de análise de conformidade. Acreditamos que o processo será concluído com sucesso, pois o bom funcionamento do ASI-HSM já é comprovado no seu uso em diversas universidades brasileiras, por meio do projeto ICPEDU.

Após o ASI-HSM receber o selo de homologação ICP-Brasil, ele estará apto a ser utilizado na AC-Raiz Brasileira e qualquer instituição no âmbito da ICP-Brasil, assim as instituições brasileiras poderão utilizar um HSM nacional, produzido com esforços de universidades e instituições brasileiras.

O ASI-HSM recebeu vários benefícios com a homologação além do selo ICP-Brasil. Agora o ASI-HSM possui uma vasta documentação técnica de seu projeto e de suas funcionalidades. Várias melhorias foram implementadas, que garantiram maior robustez e segurança ao conteúdo armazenado no módulo. A documentação do usuário final foi aprimorada e a interface gráfica do usuário recebeu melhorias, se preocupando com a usabilidade do ASI-HSM.

Com o selo ICP-Brasil, o ASI-HSM ganha mais valor como um HSM de mercado, pois passou por um processo de controle de qualidade que qualquer outro HSM passaria para receber o selo.

Um dos mais beneficiados com a homologação é o projeto ICPEDU e as

universidades brasileiras que estão ligadas ao projeto, pois a utilização de um HSM comprovadamente seguro e funcional engrandece o projeto, na medida que os envolvidos com as questões de operação de uma AC receberão treinamento e capacitação com o ASI-HSM homologado ICP-Brasil.

Referências

- [Adv 09] Advanced Micro Devices, Inc. **AMD Connectivity Solutions - AMD GeodeTM Processor Family**. Disponível em <http://www.amd.com/us-en/ConnectivitySolutions/ProductInformation/0,,50_2330_9863,00.html>. Acesso em: 4 de dezembro de 2009.
- [CCI 09] CCID. **CCID free software driver**. Disponível em <<http://pcslite.alioth.debian.org/ccid.html>>. Acesso em: 4 de dezembro de 2009.
- [Com 09] Communications Security Establishment Canada. **Communications Security Establishment Canada Homepage**. Disponível em <<http://www.cse-cst.gc.ca/index-eng.html>>. Acesso em: 4 de dezembro de 2009.
- [dS 08] DE SOUZA, T. C. S.; MARTINA, J. E.; CUSTÓDIO, R. F. Audit and backup procedures for hardware security modules. In: IDTRUST, 2008. **Proceedings...** Gaithersburg, Maryland, USA: [s.n.], 2008. p.89–97.
- [Eur 09] EuroPKI. **EuroPKI**. Disponível em <<http://www.europki.org>>. Acesso em: 4 de dezembro de 2009.
- [Fre 09a] FreeBSD System Calls Manual. **UNIX man pages : chroot (2)**. Disponível em <http://www-sbras.nsc.ru/cgi-bin/www/unix_help/unix-man?chroot+2>. Acesso em: 4 de dezembro de 2009.
- [Fre 09b] FreeBSD System Manager's Manual. **FreeBSD man pages : fsck (8)**. Disponível em <<http://www.manpages.info/freebsd/fsck.8.html>>. Acesso em: 4 de dezembro de 2009.
- [ICP 09] ICPEDU. **ICPEDU**. <https://www.icp.edu.br>.
- [Inf 09a] Infra-estrutura de Chaves Públicas Brasileira. **Formulário de requerimento de homologação de sistemas e equipamento de certificação digital no âmbito da ICP-Brasil**. Disponível em <<http://www.iti.gov.br/twiki/pub/Homologacao/Documentos/ADE-ICP-1001C-v20.doc>>. Acesso em: 4 de dezembro de 2009.

- [Inf 09b] Infra-estrutura de Chaves Públicas Brasileira. **Laboratórios Credenciados**. Disponível em <<http://www.iti.gov.br/twiki/bin/view/Homologacao/LaboratoriosCredenciados>>. Acesso em: 4 de dezembro de 2009.
- [Inf 09c] Infra-estrutura de Chaves Públicas Brasileira. **Manual de Condutas Técnicas 7 - Volume I: Requisitos, Materiais e Documentos Técnicos para Homologação de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP-Brasil**. Disponível em <http://www.iti.gov.br/twiki/pub/Homologacao/Documentos/MCT7_-_Vol.I.pdf>. Acesso em: 4 de dezembro de 2009.
- [Inf 09d] Infra-estrutura de Chaves Públicas Brasileira. **Modelo de termo de propriedade intelectual**. Disponível em <<http://www.iti.gov.br/twiki/pub/Homologacao/Documentos/ADE-ICP-1001A-v20.doc>>. Acesso em: 4 de dezembro de 2009.
- [Inf 09e] Infra-estrutura de Chaves Públicas Brasileira. **Modelo de termo de sigilo**. Disponível em <<http://www.iti.gov.br/twiki/pub/Homologacao/Documentos/ADE-ICP-1001B-v20.doc>>. Acesso em: 4 de dezembro de 2009.
- [Ins 09a] Instituto de Tecnologia da Informação. **ICP-Brasil**. Disponível em <<http://www.iti.gov.br/twiki/bin/view/Certificacao/WebHome>>. Acesso em: 4 de dezembro de 2009.
- [Ins 09b] Instituto de Tecnologia da Informação. **Instituto de Tecnologia da Informação**. Disponível em <<http://www.iti.gov.br/>>. Acesso em: 4 de dezembro de 2009.
- [Int 09] Internet2. **Symposium on Identity and Trust on the Internet (IDtrust Symposiums)**. Disponível em <<http://middleware.internet2.edu/idtrust/>>. Acesso em: 4 de dezembro de 2009.
- [Kry 09] Kryptus. **KRYPTUS - Engenharia Criptográfica**. Disponível em <<http://www.kryptus.com>>. Acesso em: 4 de dezembro de 2009.
- [Lab 09a] LabSEC. **ASI-HSM**. <https://projetos.labsec.ufsc.br/openshsmd>.
- [Lab 09b] LabSEC. **Laboratório de Segurança em Computação**. Disponível em <<http://www.labsec.ufsc.br>>. Acesso em: 4 de dezembro de 2009.
- [lib 09] libusb project. **libusb**. Disponível em <<http://libusb.org/>>. Acesso em: 4 de dezembro de 2009.
- [MAR 07] MARTINA, J. E.; DE SOUZA, T. C. S.; CUSTÓDIO, R. F. Openshm: An open key life cycle protocol for public key infrastructure's hardware security modules. In: EUROPKI, 2007. **Proceedings...** Palma de Mallorca, Spain: [s.n.], 2007. p.220–235.

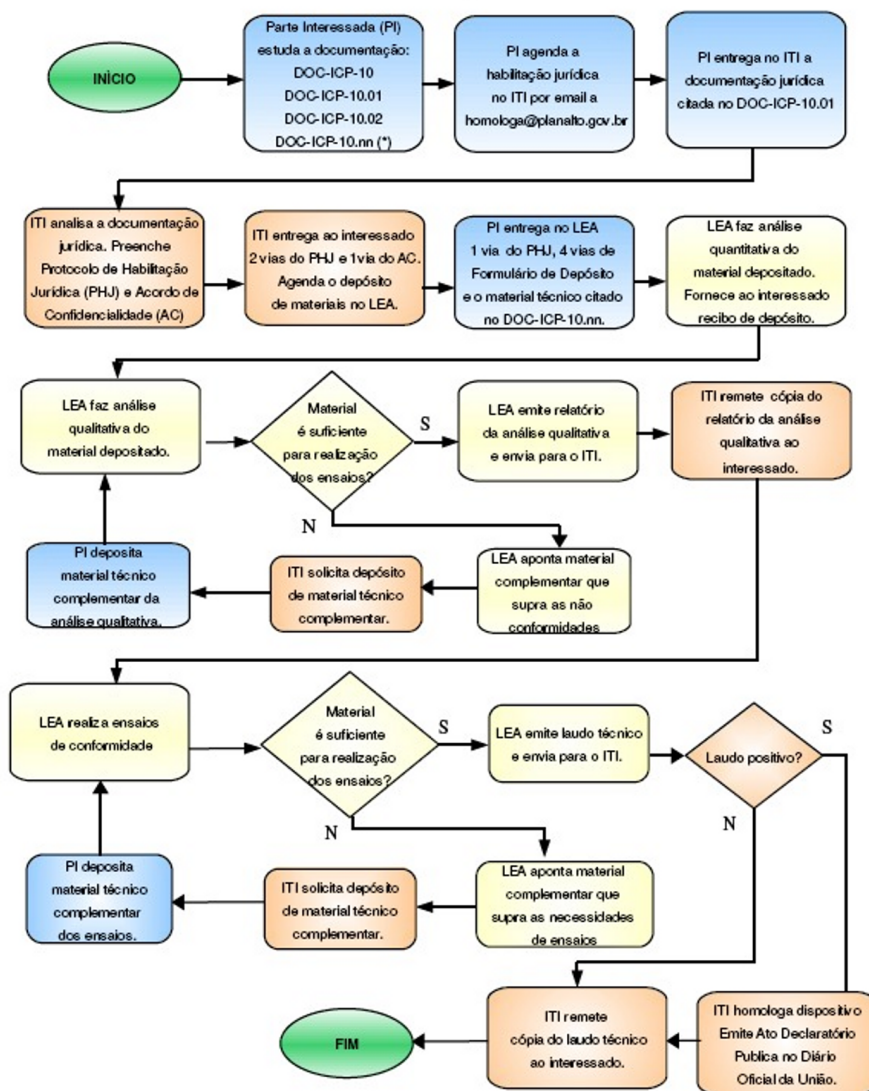
- [Nat 09a] National Institute of Standards and Technology. **National Institute of Standards and Technology**. Disponível em <<http://www.nist.gov/>>. Acesso em: 4 de dezembro de 2009.
- [Nat 09b] National Institute of Standards and Technology. **NIST and Industry**. Disponível em <http://www.nist.gov/public_affairs/industry.htm>. Acesso em: 4 de dezembro de 2009.
- [Nat 09c] National Institute of Standards and Technology. **NIST.gov - Computer Security Division - Computer Security Resource Center**. Disponível em <<http://csrc.nist.gov/groups/STM/cmvp/index.html>>. Acesso em: 4 de dezembro de 2009.
- [Ope 09a] Open Source Software Institute. **OpenSSL FIPS Object Module**. Disponível em <<http://www.openssl.org/docs/fips/UserGuide-1.2.pdf>>. Acesso em: 4 de dezembro de 2009.
- [Ope 09b] OpenBSD. **OpenSSH**. Disponível em <<http://www.openssh.com/>>. Acesso em: 4 de dezembro de 2009.
- [Ope 09c] OpenSC project. **OpenCT**. Disponível em <<http://www.opensc-project.org/openct/>>. Acesso em: 4 de dezembro de 2009.
- [Ope 09d] OpenSC project. **opensc-project.org Home of open source smart card solutions**. Disponível em <<http://www.opensc-project.org/>>. Acesso em: 4 de dezembro de 2009.
- [PC 09a] PC Engines. **PC Engines ALIX system boards**. Disponível em <<http://www.pcengines.ch/alix.htm>>. Acesso em: 4 de dezembro de 2009.
- [PC 09b] PC Tech FAQ. **O que é um shell Unix?** Disponível em <<http://pt.tech-faq.com/unix-shell.shtml>>. Acesso em: 4 de dezembro de 2009.
- [PCS 09] PCSC-Lite. **PCSC-Lite Home page on Alioth**. Disponível em <<http://pcslite.alioth.debian.org/>>. Acesso em: 4 de dezembro de 2009.
- [RNP 09] RNP. **Rede Nacional de Ensino e Pesquisa**. Disponível em <<http://www.rnp.br>>. Acesso em: 4 de dezembro de 2009.
- [SCH 96] SCHNEIER, B. **Applied Cryptography**. John Wiley & Sons, 1996.
- [SQL 09] SQLite. **SQLite Home Page**. Disponível em <<http://www.sqlite.org/>>. Acesso em: 4 de dezembro de 2009.
- [Sun 09] Sun Microsystems. **Java**. Disponível em <<http://www.java.com/>>. Acesso em: 4 de dezembro de 2009.
- [The 09a] The FreeBSD Project. **About FreeBSD Ports**. Disponível em <<http://www.freebsd.org/ports/>>. Acesso em: 4 de dezembro de 2009.

- [The 09b] The FreeBSD Project. **The FreeBSD Project**. Disponível em <<http://www.freebsd.org/>>. Acesso em: 4 de dezembro de 2009.
- [The 09c] The OpenSSL Project. **OpenSSL: Documents, engine(3)**. Disponível em <<http://www.openssl.org/docs/crypto/engine.html>>. Acesso em: 4 de dezembro de 2009.
- [The 09d] The OpenSSL Project. **OpenSSL: The Open Source toolkit for SSL/TLS**. Disponível em <<http://www.openssl.org/>>. Acesso em: 4 de dezembro de 2009.
- [X.O 09] X.Org Foundation. **X.Org**. Disponível em <<http://www.x.org/wiki/>>. Acesso em: 4 de dezembro de 2009.

Apêndice A

Etapas do Processo de Homologação

VISÃO GERAL DO PROCESSO DE HOMOLOGAÇÃO NA ICP-BRASIL - v.1.0 - 20.12.2007



(*) O número do DOC-ICP-10.nn depende do tipo de dispositivo a homologar:

DOC-ICP.10.03 - CARTÕES INTELIGENTES, LEITORAS E TOKENS CRIPTOGRÁFICOS

DOC-ICP.10.04 - SOFTWARES DE ASSINATURA DIGITAL, SIGILO E AUTENTICAÇÃO

DOC-ICP.10.05 - MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA (MSC)

DOC-ICP.10.06 - SOFTWARES PARA BIBLIOTECAS CRIPTOGRÁFICAS E PROVEDORES DE SERVIÇOS CRIPTOGRÁFICOS

Figura A.1: Fluxograma do Processo de Homologação

Apêndice B

Diagramas de Estados

B.1 Diagrama Geral de Estados

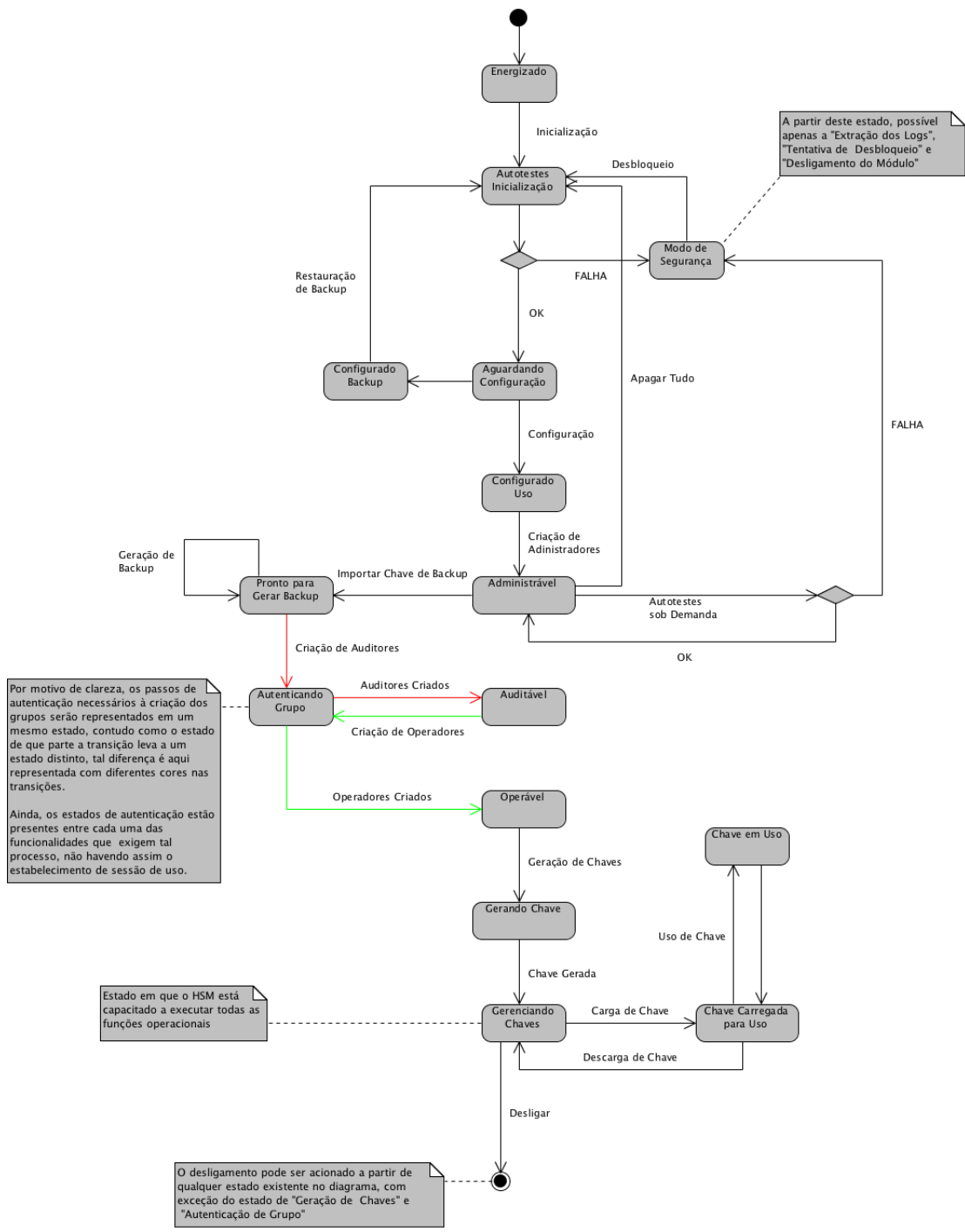


Figura B.1: Diagrama de estados do ASI-HSM

B.2 Diagrama de Inicialização e Gerência de Perfis

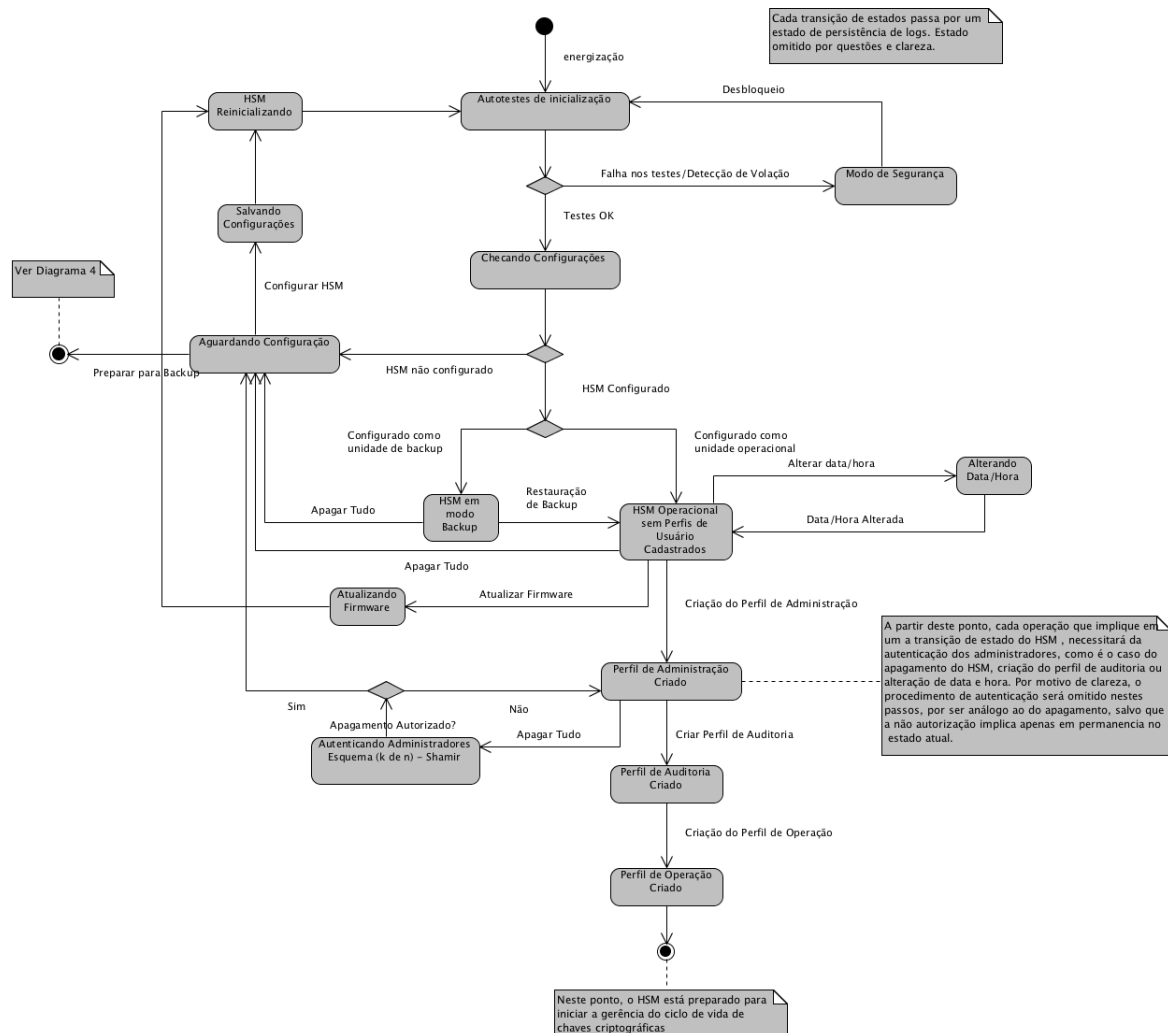


Figura B.2: Diagrama de estados detalhando a inicialização e criação dos perfis do ASI-HSM

B.3 Diagramas de Geração e Uso de Chaves

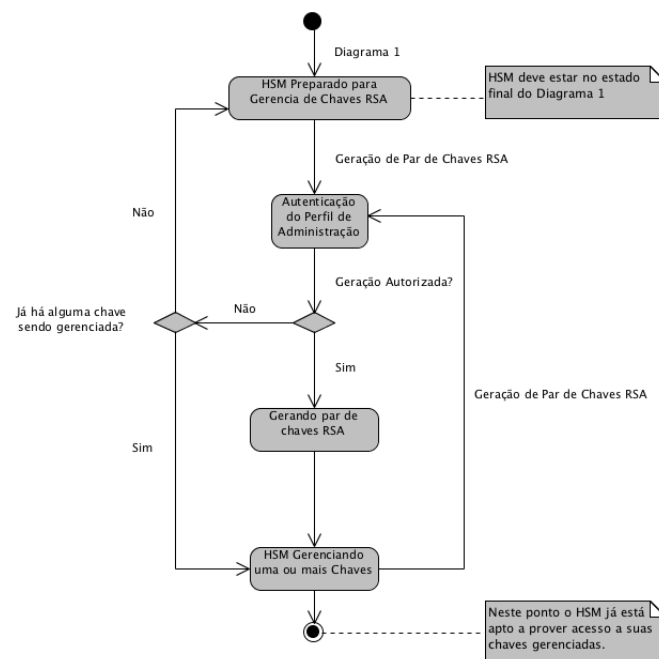


Figura B.3: Diagrama de estados detalhando a criação de chaves do ASI-HSM.

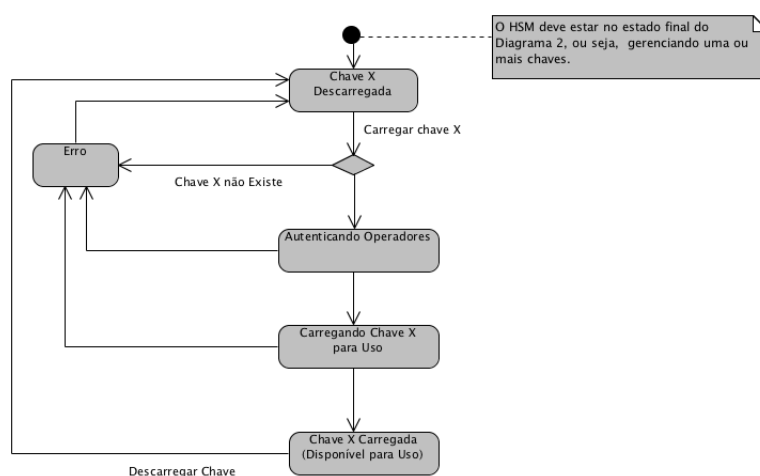


Figura B.4: Diagrama de estados detalhando a liberação e uso de chaves gerenciadas pelo ASI-HSM.

B.4 Diagramas relacionados ao Esquema de Backup

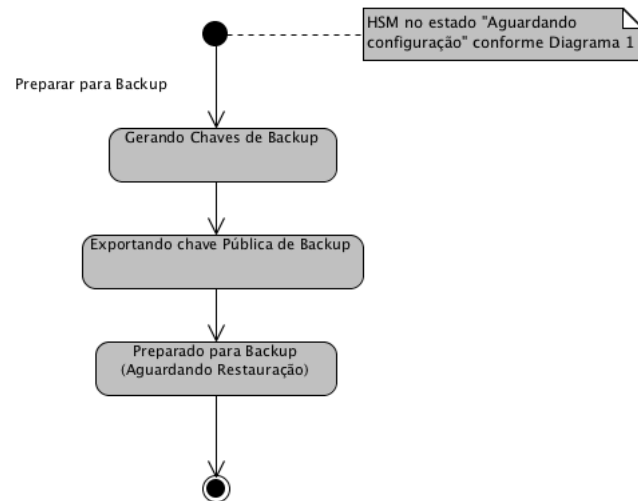


Figura B.5: Diagrama de estados detalhando a configuração do ASI-HSM como unidade de backup.

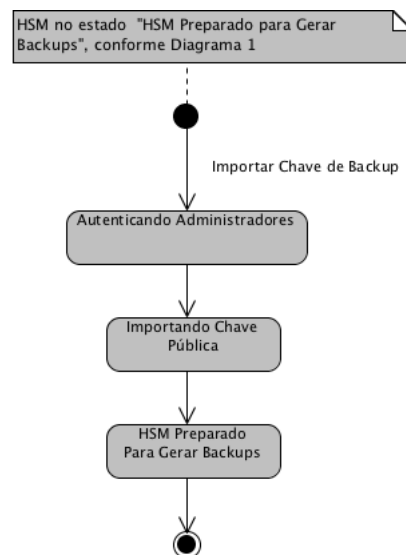


Figura B.6: Diagrama de estados detalhando a importação de chaves de backup.

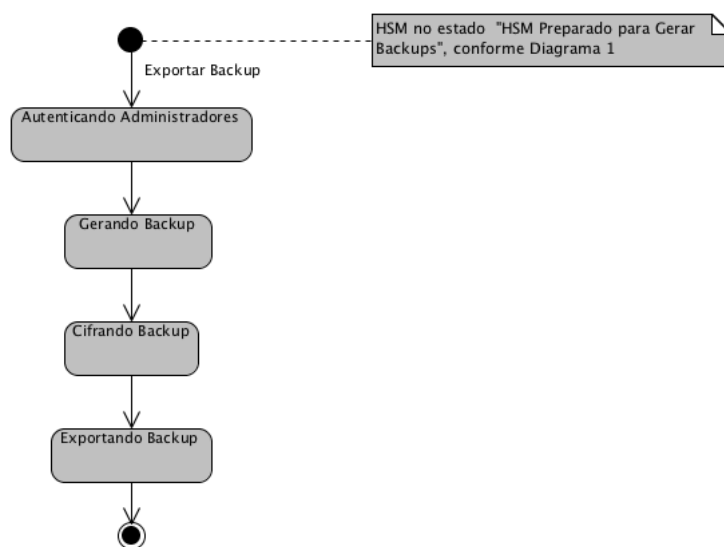


Figura B.7: Diagrama de estados detalhando a geração de backups de um ASI-HSM em operação.

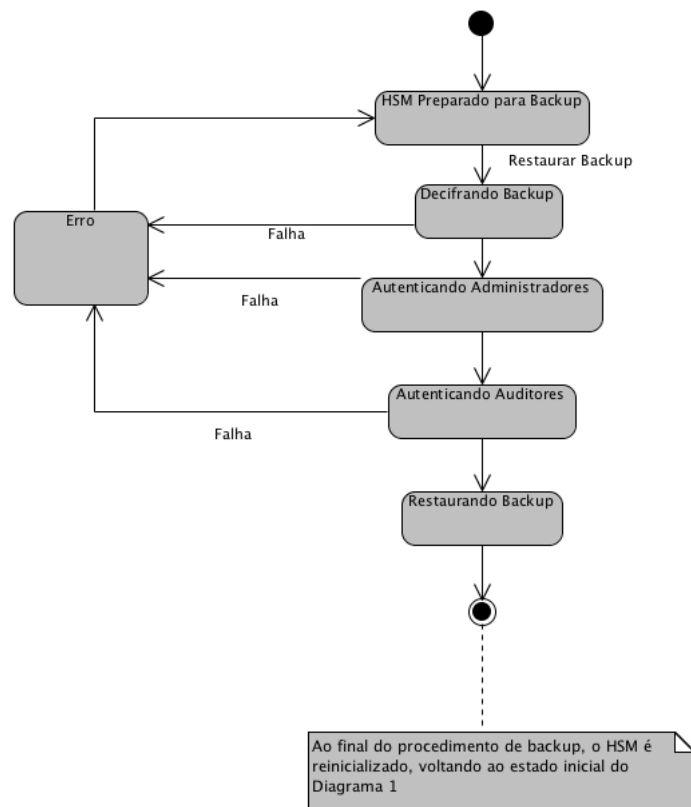


Figura B.8: Diagrama de estados detalhando a restauração de backup em um ASI-HSM préconfigurado.