UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

Túlio Cícero Salvaro de Souza

Aplicações Embarcadas para Gerenciamento de Chaves Criptográficas

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

Jean Everson Martina, Msc

Prof. Ricardo Felipe Custódio, Dr.

Florianópolis, Junho de 2005

Aplicações Embarcadas para Gerenciamento de Chaves Criptográficas

Túlio Cícero Salvaro de Souza

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Bacharel em Sistemas de Informação, área de concentração Sistema de Computação e aprovado em sua forma final pelo Programa de Graduação em Sistemas de Informação.

Prof. Olinto José Varella Furtado, Dr.
Coordenador do Curso

Banca Examinadora

Jean Everson Martina, Msc

Prof. Ricardo Felipe Custódio, Dr.

Júlio da Silva Dias, Dr.

Prof. Daniel Santana de Freitas, Dr.

"Cada um com seus problemas!"

Jean Everson Martina - 2004/2005

Ofereço este trabalho a muitas pessoas: meu pai, minha mãe, minha namorada ...

Agradecimentos

Primeiramente, gostaria de agradecer a meus pais, os principais responsáveis pelo que sou hoje, por muito apoio, incentivo e ajuda.

Ao Professor Custódio, desejo agradecer por abrir a oportunidade e confiar no meu trabalho. Ao Jean, pelo tempo despendido com as correções e ajudas, tanto na implementação, quando na escrita.

Ao pessoal do LabSEC, Júlio, Martin, Paulo, Douglas e ao Professor Daniel queria demonstrar minha gratidão pelas dúvidas retiradas e pela atenção dispensada.

Apesar de não estar ligado diretamente ao projeto, também manifesto a minha gratidão a quem sempre me incentivou e deu a idéia de entrar em contato com o LabSEC, o Professor Olinto José Varela Furtado.

Eu agradeço pelos momentos felizes e, porque não, os tristes? Minha gratidão a todos que deles compartilharam.

E o agradecimento final a minha namorada, que aguentou a minha falta de tempo, dedicação e, acima de tudo, muitos momentos longe da sua família. Sem sombra de dúvidas, uma das pessoas que mais sofreu durante este projeto.

Sumário

Sumário vi

Lista de Figuras ix

Lista de Siglas x

Lista de Símbolos xii

Resumo xiii

Abstract xiv

1 Introdução 1

1.1 Criptografia 1

1.1.1 Criptografia Simétrica 2

1.1.2 Funções de Resumos Criptográficos 2

1.1.3 Criptografia Assimétrica 3

1.1.4 Certificados Digitais e Infra-estrutura de Chaves Públicas 3

1.2 Provedor de Serviços Criptográficos 5

1.3 Objetivos 6

1.3.1 Objetivo Geral 6

1.3.2 Objetivos Específicos 6

1.4 Justificativa e Motivação 7

1.5 Trabalhos Relacionados 7

1.6 Estrutura do trabalho 8

2 Mecanismos para Gerenciamento de Chaves Criptográficas 10

2.1 Criação de Administradores 11

2.2 Criação do Conjunto de Operadores 14
2.3 Criação de Pares de Chaves Assimétricas 17
2.4 Utilização de Pares de Chaves Assimétricas 19
2.5 Troca de Administradores 20
2.6 Troca de Operadores para uma Chave Assimétrica 23
2.7 Sistema para Cópia de Segurança 25
2.8 Recuperação de Cópia de Segurança 28
2.9 O Conjunto de Auditores 31

3 Definição da Aplicação e Problemas Enfrentados 33
3.1 Linguagem Adotada 33
3.2 Comunicação e Forma de Execução da Aplicação Gestora 34
3.3 Dispositivo de Armazenamento de Usuários 35
3.4 Bibliotecas Utilizadas 36
3.4.1 POSIX Thread 36
3.4.2 OpenCT 37
3.4.3 OpenSC 37
3.4.4 SQLite 37
3.4.5 Share Secret 37
3.4.6 OpenSSL 38
3.5 Ambiente de Desenvolvimento 38
3.6 Sistema de Documentação 39
3.7 Problemas Enfrentados 39
3.7.1 Documentação das Bibliotecas Utilizadas 39
3.7.2 Controle de Execução de Programas 40

4 Aplicação Gestora Desenvolvida 41
4.1 Iterações com Smartcards 41
4.2 Sistema de Armazenamento 42
4.2.1 Administradores 42
4.2.2 Operadores 45
4.2.3 Chaves 46
4.2.4 Dados Não Exportáveis 47

4.2.5 Cópia de Segurança 47
4.2.6 Configurações 50
4.3 Configuração do Provedor de Serviços Criptográficos 52
4.4 Zerador do Provedor de Serviços Criptográficos 54
4.5 Criação de Administradores 55
4.6 Criação de Grupos de Operadores 56
4.7 Troca de Administradores 58
4.8 Troca de Grupo de Operadores 59
4.9 Criação de Pares Chaves 60
4.10 Utilização dos Pares de Chaves 61
4.11 Cópia de Segurança 62
4.12 Recuperação da Cópia de Segurança 63
4.13 Funções Auxiliares 66
4.13.1 Listagem dos Grupos de Operadores 66
4.13.2 Listagem dos Operadores de um Grupo 66
4.13.3 Listagem das Chaves Gerenciadas 66
4.13.4 Ativação dos Conjuntos de Operadores 67
4.13.5 Listagem do Conteúdo de um Smartcard 67
4.13.6 Serviços Criptográficos 68

5 Conclusões **69**

Referências Bibliográficas **71**

A Anexos **74**

Lista de Figuras

2.1 Mecanismos para Criação do Conjunto de Administradores. 12
2.2 Mecanismos para Criação de Conjuntos de Operadores. 14
2.3 Mecanismos para Criação de Chaves Assimétricas 18
2.4 Mecanismos para utilização de Chaves Assimétricas 19
2.5 Mecanismos para troca do Conjunto de Administradores 21
2.6 Mecanismos para troca de Operadores para uma Chave Assimétrica . . . 23
2.7 Mecanismos para realização da Cópia de Segurança 26
2.8 Mecanismos para recuperação da Cópia de Segurança 29

Lista de Siglas

AC	Autoridade Certificadora
AG	Aplicação Gestora
AES	Advanced Encryption Algorithm (Algorítmo de Cifragem Avançada)
ANOREG-BR	Associação dos Notários e Registradores do Brasil
ANSI	American National Standards Institute (Instituto Nacional de Padrões Americanos)
API	Interface de Programação de Aplicativos (Application Program Interface)
BR	Brasil
CBC	Cipher Block Chaining (Encadeamento de Blocos Cifrados)
DES	Decryption and Encryption Standard (Padrão de Cifragem e Decifragem)
HSM	Módulo de Hardware Criptográficos
HTML	Linguagem de Marcação Hipertexto (HyperText Markup Language)
ICP	Infra-estrutura de Chaves Públicas
ICP-EDU	Infra-estrutura de Chaves Públicas Educacional
IDE	Ambiente de Desenvolvimento Integrado (Integrated Development Environment)
IEC	Internacional Electronical Commission
IEEE	Instituto de Engenharia Elétrica e Eletrônica (Institute of Electrical and Electronics Engineers)
IPSec	IP security
ISO	Internal Organization for Standardization
ITI	Instituto Nacional de Tecnologia da Informacao
LCR	Lista de Certificados Revogados

PDF	Portable Document Format
PIN	Número de Identificação Pessoal (personal identification number)
PKCS	Public Key Crypto System
PKI	Infra-estrutura de Chaves Públicas (Public key infrastructure)
PSC	Provedor de Serviços Criptográficos
PUK	Código de Desbloqueio Pessoal (Personal Unlocking Code)
RSA	Rivest, Shamir e Adelman
SHA	Secure Hash Algorithm (Algoritmo Seguro de Resumo Criptográfico)
SQL	Linguagem de Questões Estruturadas (Structured Query Language)
SSH	Secure Shell
SSL	Secure Sockets Layer
SPK	Standard with Public Key
STARCOS	Smartcard Operating System
TLS	Transport Layer Security
USB	Universal Serial Bus

Lista de Símbolos

- $\geq$ Maior ou igual que
- $\leq$ Menor ou igual que
- $\oplus$ XOR / Ou exclusivo

Resumo

Este trabalho de conclusão de curso é baseado na proposta de um Provedor de Serviços Criptográficos voltado para infra-estrutura de chaves públicas. Este tema foi abordado na dissertação de mestrado de Jean Everson Martina, sendo aprovado pela Universidade Federal de Santa Catarina. Os mecanismos de gerenciamento das chaves apresentados na tese foram implementados, servindo como ponto de partida para o presente trabalho.

O projeto provê a implementação de uma Aplicação Gestora, embarcada, que servirá de Provedor de Serviços Criptográficos, gerenciando os ciclos de chaves criptográficas de ambientes com alto valor agregado de informação, como por exemplo, uma Autoridade Certificadora.

O presente trabalho engloba as definições da Aplicação Gestora, assim como os problemas enfrentados e as razões que motivaram o rumo do protótipo. Serão descritas as bibliotecas usadas na implementação.

Na parte final, serão descritos os processos de implementação, trata-se da etapa mais importante, pois expõe a forma como os recursos e técnicas foram utilizados. As razões que comprovam sua contribuição também serão mostrados.

Na conclusão, além da síntese do projeto, a possibilidade de trabalhos futuros serão apresentados, contribuindo, assim, para o desenvolvimento de novas pesquisas na área de segurança da computação.

Palavras Chaves: Gerenciamento de Chaves Criptográficas, Criptografia Assimétrica, Infra-Estrutura de Chaves Públicas, Módulos de Segurança Criptográfica.

Abstract

This research work is based on a Criptographic Service Provider to use in Public Key Infrastructures. The main ideas of this subject were present on Jean Everson Martina's Masters Dissertation, being aprooved by the Federal University of Santa Catarina in Brazil. The key management schemes presented on this dissertation were impleented as the starting point of the present work.

This project aims in implement an embbeded Key Management Application to work as a Criptographic Service Provider, managing the life-cycle of high valuable cryptographic keys, like Certification Authorities ones.

During the work we define all terms used do implement the Key Management Application, as well the problems we faced and the reasons of some choices we made during prototipation. We also describe the programing libraries we used.

At last, we describe the processes regarding implementation. This is considered the most important part because we exposed how techniques and resources were managed to get it working. Reasons regarding to the work contributions are also showed.

Concluding the work, we sumarize the project, target some future works, trying to contribute to the development of the new area.

Keywords: Cryptographic Keys Management, Assymetric Cryptography, Public Keys Infrastructure, Hardware Security Modules.

Capítulo 1

Introdução

Nas redes computacionais atuais, a segurança da informação tornou-se uma das maiores preocupações. O ato de salvar dados no computador pessoal não assegura a privacidade dos mesmos. Por segurança da informação entende-se os requisitos de integridade, tempestividade, sigilo e confiança no armazenamento [1].

A Criptografia é uma das ferramentas existentes para prover esta segurança. Os ambientes corporativos que necessitam armazenar informações sigilosas, mais especificamente, chaves secretas, devem fazê-lo em plataformas computacionais seguras.

A busca por sistemas criptográficos de armazenamento seguro é crescente, e os Provedores de Serviços Criptográficos, PSCs, entram como a solução atual. Por PSC, entende-se um ambiente computacional capaz de executar funções criptográficas e gerenciar o ciclo de vida de chaves.

Estes ambientes são compostos por um Módulo de Hardware Criptográfico, HSM, e a Aplicação Gestora, AG. O PSC implementa, através de mecanismos de gerenciamento de chaves criptográficos, o ambiente capaz de prover a segurança requerida por estes sistemas.

1.1 Criptografia

Criptografia (Do Grego kryptós, "escondido", e gráphein, "escrever") é geralmente entendido como sendo o estudo dos princípios e das técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, a menos que seja conhecida a "chave secreta", o que a torna difícil de ser lida por alguém não

autorizado [2].

Os objetivos principais da criptografia, quando utilizados para troca de mensagens, são [2]:

- confidencialidade da mensagem: só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada;
- integridade da mensagem: o destinatário deverá ser capaz de determinar se a mensagem foi alterada durante a transmissão;
- autenticação do remetente: o destinatário deverá ser capaz de identificar o remetente e verificar que foi mesmo ele quem enviou a mensagem;
- não-repúdio do remetente: não deverá ser possível ao remetente negar o envio da mensagem.

Nem todos os sistemas ou algoritmos criptográficos atingem todos os objetivos listados acima. Na maioria dos casos, há a união de algumas técnicas para prover segurança.

1.1.1 Criptografia Simétrica

A criptografia simétrica é uma técnica que se utiliza a mesma chave para cifrar e decifrar uma mensagem para a qual se deseja autenticidade e confidencialidade.

A deficiência deste algoritmo para troca de mensagens entre duas partes, é que elas precisam combinar a chave que será utilizada no processo. Muitas vezes esse meio de transmissão não é seguro, comprometendo o sigilo.

1.1.2 Funções de Resumos Criptográficos

Funções de Resumos Criptográficos são versões resumidas de qualquer texto submetido a essa técnica, que garantem integridade quando usadas na forma de caminho único, as quais têm as seguintes características [3]:

- Ser computacionalmente inviável recriar a mensagem original a partir do resultado da função;

- Ser computacionalmente inviável construir duas mensagens diferentes com a mesma saída da função.

Essa técnica gera um conjunto de bits que referencia unicamente uma mensagem, considerado a impressão digital de documentos. Este conjunto de bits possui tamanho fixo para cada algoritmo de resumo utilizado.

1.1.3 Criptografia Assimétrica

A história da Criptografia teve um marco importante com o descoberta da criptografia assimétrica que permitiu uma mudança de enfoque da Criptografia [4].

A Criptografia de chave pública ou Criptografia assimétrica é um método que utiliza um par de chaves, uma chave pública e uma chave privada. A chave pública pode ser distribuída livremente, enquanto a chave privada deve ser de conhecimento apenas de seu dono.

Em um dos algoritmos de criptografia assimétrica, o RSA [5], uma mensagem cifrada com a chave pública pode somente ser decifrada pela sua chave privada correspondente. Do mesmo modo, uma mensagem cifrada com a chave privada pode somente ser decifrada pela sua chave pública correspondente.

Os algoritmos de chave pública podem ser utilizados para autenticidade, confidencialidade e não-repúdio.

Para a confidencialidade, a chave pública é usada para cifrar mensagens, que apenas o dono da chave privada pode decifrar.

Para a autenticidade, a chave privada é usada para cifrar mensagens ou mensagens resumos, com isso garante-se que apenas o dono da chave privada poderia ter cifrado a mensagem que pode ser decifrada pela chave pública.

O não-repúdio é garantido, através de uma assinatura realizada através da chave privada que tem sinergia com a chave pública, contida em um certificado digital.

1.1.4 Certificados Digitais e Infra-estrutura de Chaves Públicas

Um certificado de chave pública, normalmente denominado certificado digital, é uma declaração assinada digitalmente que estabelece uma ligação de valor de uma chave pública com a identidade da pessoa, dispositivo ou serviço que contém a chave

privada correspondente. A maioria dos certificados de uso comum se baseia no padrão de certificado X.509v3 [6].

Os certificados Digitais podem ser comparados com cartões de crédito. A diferença é que cartões de crédito relacionam um número, uma validade e uma assinatura a uma pessoa e certificados digitais relacionam uma identificação com uma chave pública.

Infra-estrutura de Chave Pública, geralmente abreviada como PKI (Public Key Infrastructure), é um sistema de certificados digitais, autoridades de certificação e outras autoridades de registro que verificam e autenticam a validade de cada parte envolvida em uma transação eletrônica, usando a criptografia de chave pública (assimétrica) [7].

Os certificados podem ser emitidos para diversos fins, como por exemplo, autenticação de usuários da Web, autenticação de servidores Web, e-mail seguro (usando extensões multipropósito do Internet Mail protegidas ou S/MIME) [8], segurança do protocolo IP (IPSec) [9], segurança da camada de transporte (TLS) [10], assinatura de código, etc. Os certificados também são emitidos de uma autoridade de certificação para outra, a fim de estabelecer uma hierarquia de certificação.

Aquele que recebe o certificado é considerado a entidade do certificado. O emissor e assinante do certificado é uma autoridade certificadora.

Normalmente, os certificados contêm as seguintes informações [11]:

- O valor da chave pública da entidade;
- As informações sobre a entidade, como nome e endereço de e-mail da entidade do certificado;
- O período de validade (período de tempo durante o qual o certificado é considerado válido);
- Informações sobre a identidade do emissor;
- A assinatura digital do emissor, que atesta a validade do vínculo entre a chave pública da entidade e as informações de identificação da entidade.

Um certificado só é válido pelo período de tempo nele especificado; cada certificado contém datas "válido de"e "válido até", que definem o período de vali-

dade. Quando o período de validade de um certificado termina, a entidade do certificado vencido deve solicitar um novo certificado.

Se for preciso desfazer o vínculo declarado em um certificado, esse pode ser revogado pelo emissor. Cada emissor, AC, mantém uma lista de certificados revogados, LCR, que pode ser usada pelos programas para verificar a validade de um determinado certificado.

Uma das principais vantagens dos certificados é que os equipamentos não têm mais que manter um conjunto de senhas para entidades individuais que precisam ser autenticadas para obterem acesso. Em vez disso, o equipamente simplesmente deposita confiança em um emissor de certificados.

O ato de um equipamento confiar em uma autoridade certificadora, prevê a confiança nas diretivas usadas para estabelecer os vínculos dos certificados emitidos por esta AC. As ACs são responsáveis pela validação dos dados contidos nos certificados emitidos por ela e por atestar que o dono do certificado possui a chave privada correspondente à chave pública.

Pode existir uma hierarquia de ACs, formada por uma AC-Raiz e demais ACs subordinadas. As ACs intermediárias ou subordinadas serão confiáveis se no caminho de certificação existir uma AC confiável e, também, existirem repositórios de certificados de todos os nodos do caminho, até chegar na AC confiável.

1.2 Provedor de Serviços Criptográficos

Um Provedor de Serviços Criptográficos (PSC) é um dispositivo de processamento criptográfico e gestão de chaves criptográficas que mantém conformidade com as normas de construção de hardware, levando em consideração os mais diversos ataques aos processos que ele protege e, assim, garantindo a sua segurança e a salvaguarda dos parâmetros críticos de segurança por ele protegidos [12].

A construção de um PSC consiste em três projetos básicos:

- Projeto Físico - o hardware que irá prover os serviços criptográficos de forma segura, utilizando os mais diferentes tipos de sensores, sendo capaz de detectar e responder a qualquer tipo de ataque;

- Projeto Lógico - engloba o sistema operacional que irá gerenciar a execução da

Aplicação Gestora em conformidade com o hardware;

- Projeto de Testes - uma política de testes capazes de reconstruir todos os possíveis ambientes e formas de ataque, garantindo uma análise segura.

A aplicação gestora implementa mecanismos de gerenciamento de chaves que geram, protegem e destroem chaves do PSC, aplicando requisitos, verificações internas de estados e controles de segurança.

Um PSC deve prover os seguintes requisitos funcionais [12]:

- Propiciar a geração de chaves assimétricas de criptografia em hardware próprio;
- Gerenciar as chaves geradas, no seu uso, armazenamento e destruição;
- Proteger as chaves privadas em sua posse, do ambiente externo ao equipamento, de forma que as mesmas não possam ser indevidamente utilizadas;
- Possuir mecanismos de evidência e resposta à intrusão ou utilização indevida;
- Possuir resistência física a ataques em seu revestimento;
- Ter processamento suficiente para a operação em uma autoridade certificadora;
- Comunicar-se de forma cifrada com o meio externo;

1.3 Objetivos

1.3.1 Objetivo Geral

Desenvolvimento de uma aplicação embarcada que servirá de Provedor de Serviços Criptográficos para o gerenciando de chaves criptográficas, para ambientes de alto valor agregado da informação, isto é, que envolvam pessoas e negociações.

1.3.2 Objetivos Específicos

- Prover um protótipo funcional para demonstração do protocolo;
- Contribuir para o desenvolvimento tecnológico do Brasil por estar participando de um projeto de âmbito nacional;

- Contribuir para a comunidade de software livre, disponibilizando a aplicação desenvolvida e cooperação na documentação das bibliotecas utilizadas;
- Agregar grande conhecimento de segurança computacional para continuar a atuar na área;
- Compreensão do desenvolvimento de sistemas embarcados;
- Estudo da linguagem de programação C;
- Aprender a utilizar bibliotecas de criptografia;
- Trabalhar com smartcards, provendo capacidade de autenticação na utilização dos mesmos.

1.4 Justificativa e Motivação

A carência do mercado brasileiro e o atual incentivo do governo federal no desenvolvimento de um Provedor de Serviços Criptográficos voltado para Infra-estrutura de Chaves Públicas, motivaram o desenvolvimento do projeto. Justifica-se esse interesse devido aospelos altos preços cobrados pelos PSCs, existentes no mercado, e pelo fato de não serem voltados para o problema proposto. A transparência das operações é seriamente afetada com o uso destes equipamentos, os quais impedem qualquer procedimento de auditoria por serem softwares proprietários.

O esforço do trabalho é adquirir conhecimento para o governo brasileiro sobre o real funcionamento de um Provedor de Serviços Criptográficos. O estudo é focado para uso em Infra-estruturas de Chaves Públicas, mas pode ser facilmente adaptado para uso em qualquer componente da ICP e, também, em aplicações que dependem dela.

1.5 Trabalhos Relacionados

A idéia de Provedor de Serviços Criptográficos vem-se difundindo pelo país, proporcionando muitas pesquisas na área e projetos reais de desenvolvimento. Entre eles, encontram-se as iniciativas da ANOREG-BR [13], Kryptus Tecnologias [14] e o

próprio governo Brasileiro, na figura do Instituto Nacional de Tecnologia da Informação, ITI [15].

O Brasil instituiu, em 2001, a ICP-Brasil [16] como raiz única de uma ICP hierárquica que iria ditar os ritmos de certificação no país. A implantação utilizou uma solução proprietária estrangeira para ICPs, o que levantou, entre outras, as seguintes questões:

- a seriedade da solução adquirida;
- o modo de operação do equipamento;

Pensando nisso, em outubro de 2003, o ITI lançou um projeto de Desenvolvimento de um Provedor de Serviços Criptográficos e um sistema Gestor de Certificados capazes de suprir todas as necessidades da AC-Raiz da ICP-Brasil [17]. O projeto chama-se João de Barro e encontra-se em fase de desenvolvimento, proporcionando um avanço tecnológico, abrangendo uma tecnologia até então desconhecida.

Na área acadêmica, a Rede Nacional de Pesquisa patrocinou um projeto de desenvolvimento de um Sistema Gestor de Certificados de código aberto, para uso acadêmico. Este projeto teve o nome ICP-EDU [18]. Após a conclusão do sistema, passou-se a ter um novo problema, a inexistência de um ambiente computacional seguro e barato para armazenamento das chaves privadas das Autoridades Certificadoras, criadas nas instituições de ensino.

Surge, então, o projeto ICP-EDU II [19], que propôs o desenvolvimento de um Provedor de Serviços Criptográficos voltado, para o ambiente acadêmico, que seria capaz de gerenciar o ciclo de vida das chaves privadas das Autoridades Certificadoras das instituições de ensino.

Esse trabalho de conclusão de curso é a implementação prática do projeto apresentado na dissertação de mestrado de Jean Everson Martina, defendida na UFSC [20]. Nele é proposto o desenvolvimento de um Provedor de Serviços Criptográficos, incluindo a Aplicação Gestora e o Módulo de Hardware Criptográfico.

1.6 Estrutura do trabalho

Tratando do desenvolvimento de uma Aplicação Gestora, no capítulo 2, serão apresentados os mecanismos criptográficos utilizados, isto é, o protocolo que será

implementado para controle do ciclo de vida das chaves gerenciadas pelo Provedor de Serviços Criptográficos.

As definições de implementação, bibliotecas utilizadas e problemas enfrentados, serão apresentados no capítulo 3, abrangendo questões como linguagem de desenvolvimento adotada.

A aplicação desenvolvida é descrita no capítulo 4, na qual são apresentadas todas as características e modos da implementação.

Por fim, serão apresentadas a conclusão do trabalho desenvolvido juntamente com as possibilidades de trabalhos futuros, seguindo o mesmo foco de tecnologia.

Capítulo 2

Mecanismos para Gerenciamento de Chaves Criptográficas

A implementação dos mecanismos para gerenciamento de chaves criptográficas é tarefa primordial para o desenvolvimento de um provedor de serviços criptográficos, PSC. Com elas será possível compreender e justificar cada passo do PSC.

Estes mecanismos foram modelados na tese base [20] deste projeto. Foram definidos em forma de diagramas e descritos textualmente.

Os mecanismos propostos seguiram os seguintes critérios [20]:

- Deverá sempre possuir um conjunto de Administradores, os quais serão responsáveis por todas as tarefas administrativas relativas ao provedor, excetuando-se as atividades de auditoria.

- Deverá possuir um ou mais conjuntos de Operadores, os quais deterão efetivamente uma chave que será protegida pelo provedor.

- Poderá possuir inúmeras chaves assimétricas para uso em aplicação, tais como chaves de uma autoridade certificadora, sendo cada uma associada a um ou mais grupos de operadores.

- Deverá possuir, por fim, um conjunto de auditores, os quais serão responsáveis pela auditoria nos eventos ocorridos no provedor.

Seguem, abaixo, a descrição dos mecanismos de criação dos atores envolvidos no gerenciamento do PSC, como também a forma de utilização. A apresentação

será textual, com o uso de diagramas de seqüência, possibilitando maior facilidade de observação do funcionamento. Textualmente, serão explicados todos os passos percorridos.

2.1 Criação de Administradores

O provedor, após realizada a configuração inicial, antes de qualquer outra execução, deverá gerar um conjunto de administradores. Esse requisito será verificado através de checagem do estado interno do provedor.

Este processo é iniciado, informando os valores de n e m, respectivamente o número mínimo e o tamanho do conjunto de administradores do provedor. Durante o processo, são solicitados os dados para criação do certificado digital e a senha para liberar acesso ao dispositivo de armazenamento criptográfico de cada administrador.

A figura 2.1 apresenta os passos para realização deste processo. A descrição de cada um é apresentada a seguir:

1. o comando de criação do conjunto de administradores é encaminhado ao PSC. Juntamente com os valores de n e m;

2. o par de chaves do PSC é gerado, Kr_{PROV} e Ku_{PROV}, respectivamente a chave privada e a chave pública;

3. gera um certificado auto-assinado para Ku_{PROV}. Esta será a Autoridade Certificadora raiz do provedor;

4. o certificado de Ku_{PROV} é armazenado na lista de certificados confiáveis. Esta lista poderá conter certificado de Autoridades externas ao PSC, gerando uma rede de autenticação;

5. a chave de sessão, Ks_{ADM}, é gerada para o conjunto de administradores que está sendo criado;

6. a chave privada do PSC é cifrada com Ks_{ADM};

7. a chave do conjunto de administradores é dividida em m partes através do algoritmo de segredo compartilhado;

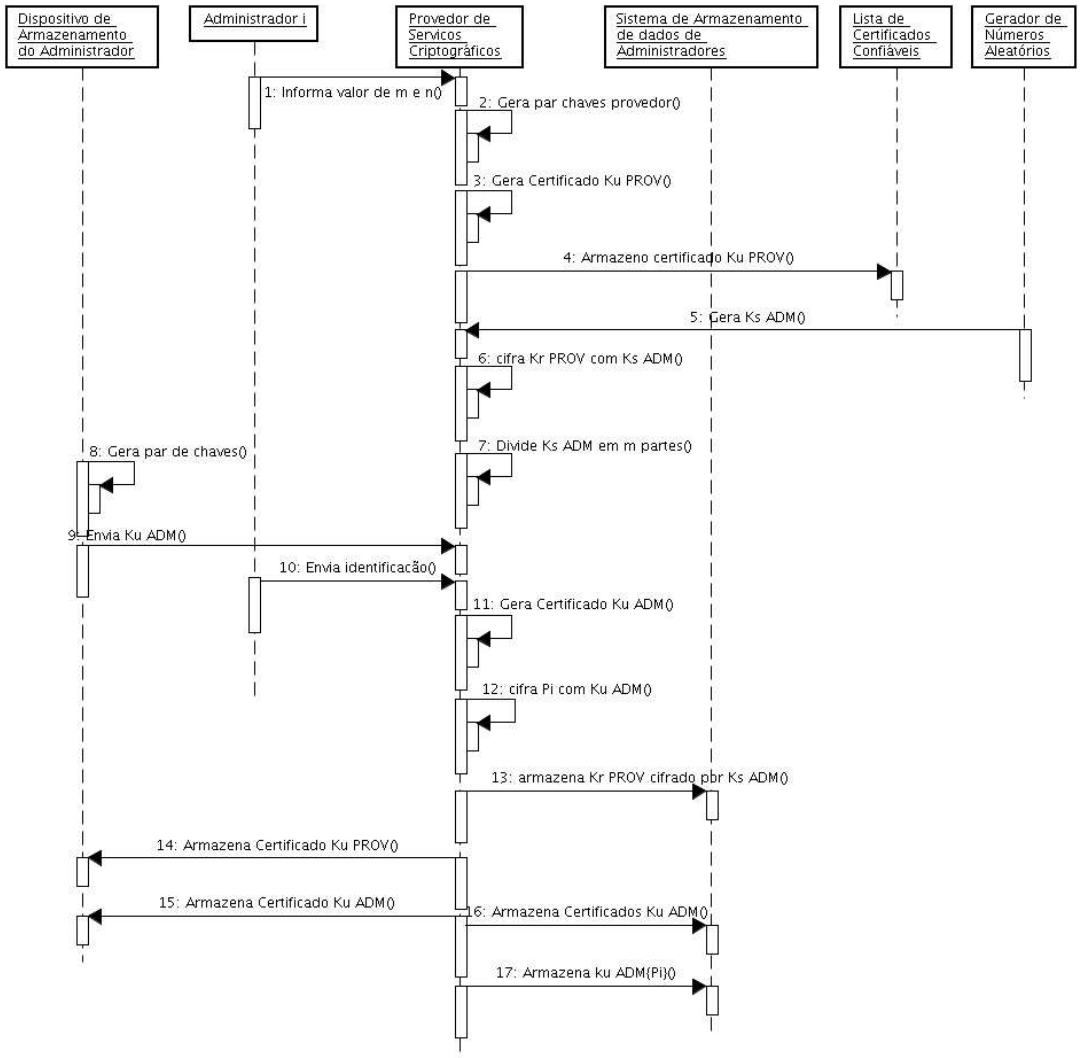

Figura 2.1: Mecanismos para Criação do Conjunto de Administradores.

8. um par de chaves é gerado no dispositivo de armazenamento de cada um dos administradores;

9. a chave pública é extraída do dispositivo de armazenamento dos administradores;

10. o administrador encaminha sua identificação ao PSC para constar no seu certificado;

11. um certificado para cada administrador é gerado, contendo as informações por ele passadas;

12. cada parte do segredo é cifrada com a chave pública de um administrador;

13. a chave privada do provedor é armazenada no sistema de armazenamento de dados dos administradores;

14. o certificado auto-assinado do provedor, gerado no passo 3, é incluído no dispositivo de armazenamento do administrador;

15. o certificado de cada administrador, gerado no passo 11, é adicionado ao seu dispositivo de armazenamento;

16. todos os certificados dos administradores são armazenados no sistema de armazenamento de administradores;

17. as partes do segredo cifradas são inseridas no sistema de armazenamento de administradores;

Os administradores, uma vez criados, são responsáveis por tarefas administrativas do provedor, as quais consistem em [20]:

- Inicialização e Operacionalização do provedor.
- Criação de Grupos de Operadores, os quais serão os detentores e utilizadores das chaves assimétricas protegidas.
- Criação de Chaves assimétricas para uso em aplicações externas ao provedor.
- Gerência de Chaves, tais como a sua delegação a um conjunto de operadores, a sua destruição ou inutilização.
- Participação de forma ativa nos procedimentos de cópias de segurança.
- Criação do Conjunto de Auditores os quais gerenciam os processos de auditoria de registro e sua legitimidade.

A utilização do Provedor de Serviços criptográficos será liberada somente após n administradores se identificarem, onde n é o valor mínimo para remontagem do segredo que cifra Kr_{PROV}. O valor de n deve respeitar a equação $1 \leq n \leq m$. Na realização da cópia de segurança do PSC (vide seção 2.7), essa regra é incrementada, a equação $1 \leq n \leq l \leq m$ deve ser respeitada neste caso, onde l representa o número mínimo para posterior recuperação da cópia de segurança.

Os administradores criados precisam realizar uma outra atividade para tornar o PSC operacional, a criação do conjunto de auditores2.9. O grupo de auditores é que vai fiscalizar e auditar todos os passos executados no interior do PSC. O estado interno do PSC não permite que nenhum outro passo possa ser executado.

2.2 Criação do Conjunto de Operadores

Continuando a operacionalização do Provedor de Serviços Criptográficos, será demonstrado agora o processo de criação do conjunto de operadores, que terá o poder de utilização dos pares de chaves assimétricas gerenciadas.

A operação inicia com a solicitação de criação de um novo conjunto de operadores ao PSC, informando o valor de k e l, respectivamente o número mínimo de operadores para recompor o segredo e o número total de componentes do conjunto. Esta é uma tarefa administrativa, necessitando a autenticação de n administradores.

Figura 2.2: Mecanismos para Criação de Conjuntos de Operadores.

A figura 2.2 apresenta os passos para realização deste processo. A descrição de cada um é apresentada a seguir:

1. o comando de criação de um conjunto de operadores é encaminhado ao PSC para disparar a execução. Os valores de k e l precisam ser informados;

2. do sistema de armazenamento de dados do administrador, carrega-se as partes do segredo dos administradores cifrados;

3. cada parte é decifrada com a chave privada contida no dispositivo de armazenamento dos administradores;

4. as partes decifradas podem reconstituir Ks_{ADM} através do algoritmo de compartilhamento de segredo;

5. a chave privada cifrada do PSC é carregada do sistema de armazenamento de administradores;

6. a decifragem de Kr_{PROV} pode ser realizada, utilizando Ks_{ADM};

7. randomicamente, as chaves $Ks_{ADM-OPER}$, Ks_{OPER} e Ks_{OPER*} são geradas. Estas chaves representam, respectivamente, a de ligação do grupo de administradores com o grupo de operadores, a do grupo de operadores é capaz de prover a rastreabilidade das chaves gerenciadas do PSC.

8. a operação lógica XOR (ou exclusivo) é realizada sobre as três chaves criadas anteriormente. O aspecto de reversibilidade do XOR é explorado nesse passo, ele consiste em aplicar a operação lógica XOR entre dois termos, A e B, obtendo como resultado C. Se novamente, aplicarmos a operação sobre C e B, obteremos A, recuperando um dos operadores iniciais.

9. o valor de Ks_{OPER*} é armazenado no sistema de armazenamento de dados não exportáveis, prevendo a rastreabilidade das chaves. A rastreabilidade é possível porque Ks_{OPER*}, uma componente do XOR de liberação de gerenciamento da chave para os administradores, é armazenado em uma base de dados Não Exportados, que em caso de realização da cópia de segurança do PSC (vide seção 2.7, obriga a reconstrução de Ks_{OPER*} com a presença dos operadores.

10. a chave $Ks_{ADM-OPER}$ é cifrada utilizando a chave pública do PSC;

11. $Ks_{ADM-OPER}$ é armazenada cifrada no sistema de armazenamento de dados de administradores;

12. o resultado da aplicação do XOR sobre as chaves, realizado no passo 8, é armazenado no sistema de armazenamento de administradores;

13. Ks_{OPER} é dividido através do algoritmo de compartilhamento de segredo em l partes;

14. um par de chaves assimétricas é gerado no dispositivo de armazenamento dos operadores, Kr_{OPER} e Ku_{OPER};

15. os operadores enviam sua identificação. Ela será usada na geração de um certificado para cada operador;

16. a chave pública dos operadores é extraída do dispositivo de armazenamento dos operadores;

17. um certificado para Ku_{OPER} é gerado com as informações enviadas pelos operadores. Ele é assinado com chave privada do PSC, Kr_{PROV};

18. cada parte do segredo é cifrada com a chave pública dos operadores;

19. o certificado de cada operador é armazenado no seu dispositivo de armazenamento;

20. o certificado auto-assinado do PSC, Ku_{PROV} é inserido no dispositivo de armazenamento dos operadores;

21. os certificados de todos os operadores são inseridos no sistema de armazenamento de dados de operadores;

22. as partes do segredo cifradas são armazenadas no sistema de armazenamento de dados de operadores;

A grande jogada do XOR, realizado no passo 8, é a possibilidade dos administradores conseguirem remontar o segredo, Ks_{OPER}, que cifra a chave gerenciada pelo PSC, permitindo a mudança dos donos das chaves. Lembrando do processo de rastreabilidade, que guarda um dos termos da operação de XOR em uma base de dados Não

Exportáveis, impossibilitando a montagem de Ks_{OPER} sem possuir Ks_{OPER*} em outro PSC.

Finalizado este processo, o Provedor de Serviços Criptográficos possui um novo conjunto de Operadores, podendo então, gerar um par de chaves (vide seção 2.3) e delegar a sua propriedade a este conjunto.

2.3 Criação de Pares de Chaves Assimétricas

A criação de pares de chaves assimétricas é mais uma tarefa administrativa, que gera chaves que serão gerenciadas pelo Provedor de Serviços Criptográficos e atribuídas a um conjunto de operadores já criados.

O processo inicia com a solicitação de criação de um novo par de chaves ao PSC. Sendo uma tarefa administrativa, a autenticação dos administradores é obrigatória, possibilitando o deciframento do mínimo de partes para remontagem do segredo, Ks_{ADM}, e por conseguinte, a carga de Kr_{PROV}.

A figura 2.3 apresenta os passos para realização deste processo. A descrição de cada um é apresentado a seguir:

1. o processo é iniciado com a solicitação da criação de um par de chaves ao PSC;
2. por se tratar de uma tarefa administrativa, é necessária a autenticação dos administradores, executando o processo de desafio apresentado no início do capítulo. Para cada administrador, é carregado do sistema de dados de administradores a parte do segredo cifrada;
3. a parte do segredo é decifrada pela chave privada, contida no dispositivo de armazenamento do administrador;
4. com todas as n partes, Ks_{ADM} pode ser remontado pelo algoritmo de segredo compartilhado;
5. do sistema de dados de administradores é carregada a chave privada do PSC cifrado;
6. é permitida a decifragem de Kr_{PROV}, utilizando Ks_{ADM};
7. a chave de ligação do conjunto de administradores e o conjunto de operadores é carregada. Ela está cifrada com a chave pública do PSC.

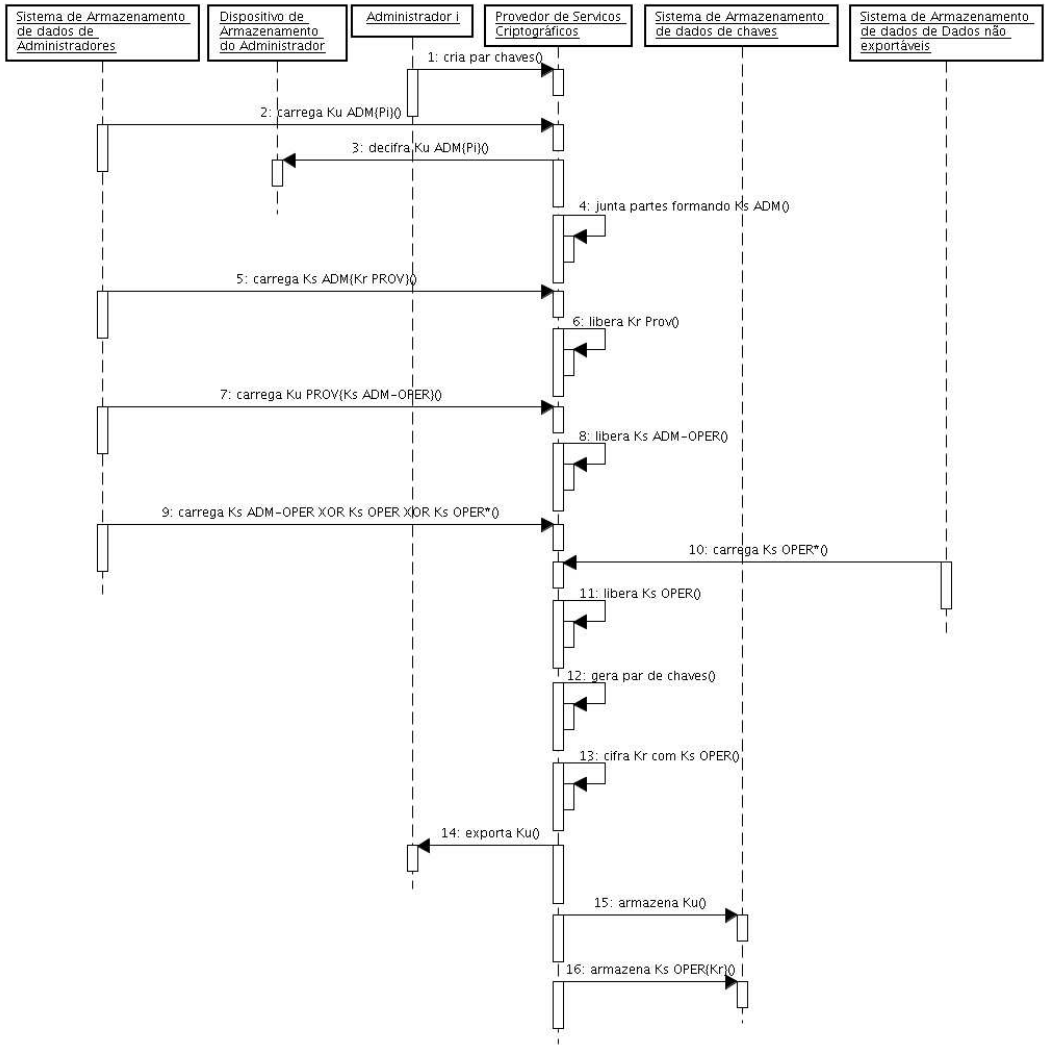

Figura 2.3: Mecanismos para Criação de Chaves Assimétricas

8. $Ks_{ADM-OPER}$ é decifrada utilizando Ks_{PROV};

9. o resultado da operação lógica XOR sobre as chaves do conjunto de operadores é carregado do sistema de armazenamento de administradores;

10. Ks_{OPER*} é carregado do sistema de armazenamento de dados não exportáveis;

11. reaplica-se a operação de XOR sobre o resultado obtido no passo 9 com as chaves Ks_{OPER*} e $Ks_{ADM-OPER}$, recuperando Ks_{OPER};

12. um par de chaves assimétricas é gerado;

13. a chave privada criada anteriormente é cifrada com a chave dos operadores, Ks_{OPER};

14. a chave pública é encaminhada para fora do PSC;

15. a chave pública é inserida no sistema de armazenamento de dados de chaves;

16. a chave privada é armazenada cifrada no sistema de armazenamento de dados de chaves;

Finalizado o processo, a chave está pronta para ser utilizada para as mais diversas funcionalidades, bastando apenas que o grupo de operadores que detém a sua posse permita. O processo de utilização do par de chaves é apresentado na seção 2.4.

2.4 Utilização de Pares de Chaves Assimétricas

A utilização dos Pares de Chaves Assimétricas é uma tarefa que envolve exclusivamente o grupo de operadores que detém o poder de uso da chave, isto é, o grupo que possui Ks_{OPER} capaz de decifrar Kr.

A solicitação de uso da chave deve ser encaminhada ao Provedor de Serviços Criptográficos, informando o par de chaves que deseja utilizar. A autenticação de k operadores será necessária, permitindo que as partes de Ks_{OPER} sejam decifrados e, conseqüentemente, remontado através do algoritmo de compartilhamento de segredo.

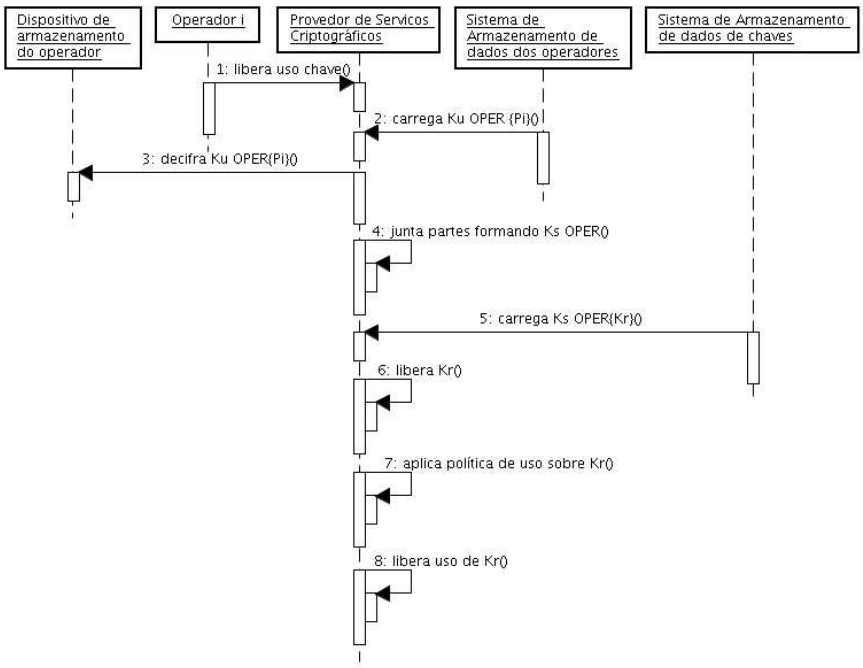

Figura 2.4: Mecanismos para utilização de Chaves Assimétricas

A figura 2.4 apresenta os passos para realização deste processo. A descrição de cada um é apresentada a seguir:

1. o processo é iniciado com solicitação de uso de uma chave ao PSC;
2. carrega do sistema de armazenamento de dados de administradores, as informações relativas as partes do segredo cifrada;
3. cada parte é decifrada com a chave privada dos operadores, Kr_{OPER} contida no seu dispositivo de armazenamento;
4. junta-se todas as partes decifradas através do algoritmo de compartilhamento de segredo, formando Ks_{OPER};
5. carrega a chave que será utilizada, do sistema de armazenamento de dados de chaves. Ela está atualmente cifrada;
6. a chave privada pode ser decifrada por Ks_{OPER};
7. aplica-se a política de uso sobre Kr;
8. a chave está pronta para ser utilizada;

As políticas de uso da chave, aplicadas no passo 7, foram estabelecidas pelos administradores no momento de sua criação. Elas determinarão se a chave será liberada para n operações criptográficas, ou por um período de tempo que poderá variar de 1 segundo a infinito.

2.5 Troca de Administradores

A troca do conjunto de administradores é uma tarefa administrativa que prevê a autenticação de n administradores. Este processo deve ser executado sempre que ocorrer o comprometimento de um sub-conjunto do conjunto de administradores $\geq n$ ou $\geq (m - n)$.

Os passos do processo de troca de administradores serão representados pelos mesmos números do diagrama de seqüência, contido na figura 2.5. A descrição é a seguinte:

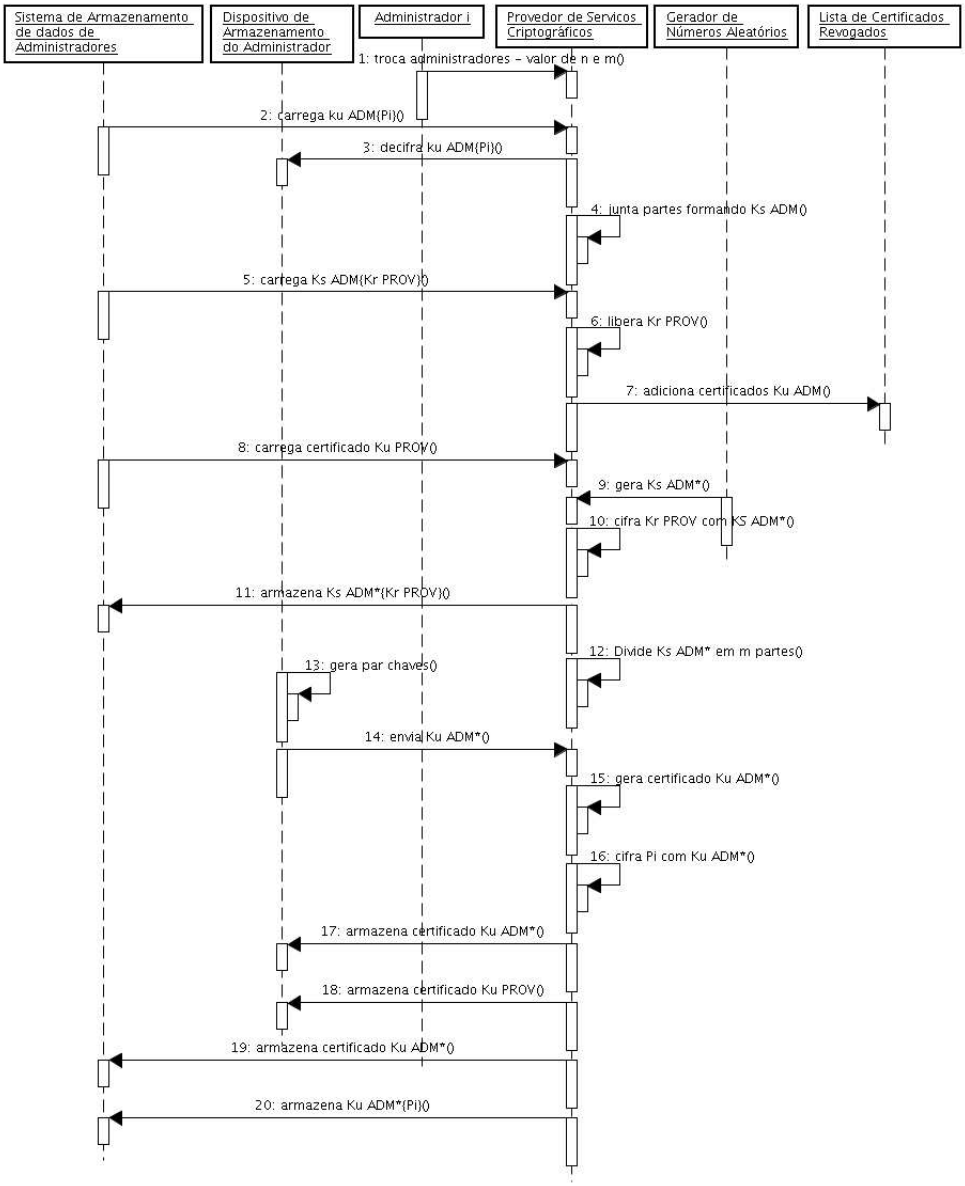

Figura 2.5: Mecanismos para troca do Conjunto de Administradores

1. a solicitação de troca do grupo de operadores é solicitada ao Provedor de Serviços Criptográficos, juntamente com o valor de n e m, respectivamente o valor mínimo para autenticação do conjunto e o número total de administradores;

2. por se tratar de uma tarefa administrativa, é necessária a autenticação dos administradores, executando o processo de desafio apresentado no início do capítulo. Para cada administrador a parte do segredo cifrado é carregada do sistema de dados de administradores;

3. a parte do segredo é decifrada pela chave privada contida no dispositivo de armaze-

namento do administrador;

4. Ks_{ADM} pode ser remontado pelo algoritmo de segredo compartilhado com todas as n partes;

5. a chave privada do PSC cifrada é carregada do sistema de dados de administradores;

6. é permitida a decifragem de Kr_{PROV} utilizando Ks_{ADM};

7. os certificados dos administradores são inseridos na lista de certificados revogados para garantir a sua invalidez;

8. carrega Ku_{PROV} do sistema de armazenamento de dados dos administradores;

9. o gerador de número aleatórios gera Ks_{ADM*}, o segredo que será usado pelo novo grupo de administradores;

10. cifra Kr_{PROV} com a chave do novo grupo de operadores, Ks_{ADM*};

11. a chave privada do PSC é armazenada no sistema de dados de administradores;

12. divide a chave Ks_{ADM*} por m, o número total do novo grupo de administradores;

13. para cada administrador é gerado um par de chaves no seu dispositivo de armazenamento, Kr_{ADM*} e Ku_{ADM*};

14. é carregada Ku_{ADM*} do dispositivo de armazenamento dos administradores;

15. gera um certificado para cada administrador assinado por Kr_{PROV};

16. utilizando Ku_{ADM*}, é cifrado cada parte do segredo dividido no item 12;

17. armazena o certificado gerado de cada administrador, Ku_{ADM*}, no seu respectivo dispositivo de armazenamento;

18. armazena o certificado do PSC no dispositivo de armazenamento de cada administrador;

19. armazena o certificado gerado de cada administrador, Ku_{ADM*}, no sistema de armazenando de dados de administradores;

20. armazena as partes cifradas do segredo no sistema de armazenamento de dados de administradores.

Este processo é idêntico ao de criação do conjunto, a diferença é a necessidade de autenticação do atual grupo de administradores.

2.6 Troca de Operadores para uma Chave Assimétrica

Este processo é a troca do conjunto de operadores que detém o poder de um par de chaves assimétricas. Os grupos já precisam estar criados.

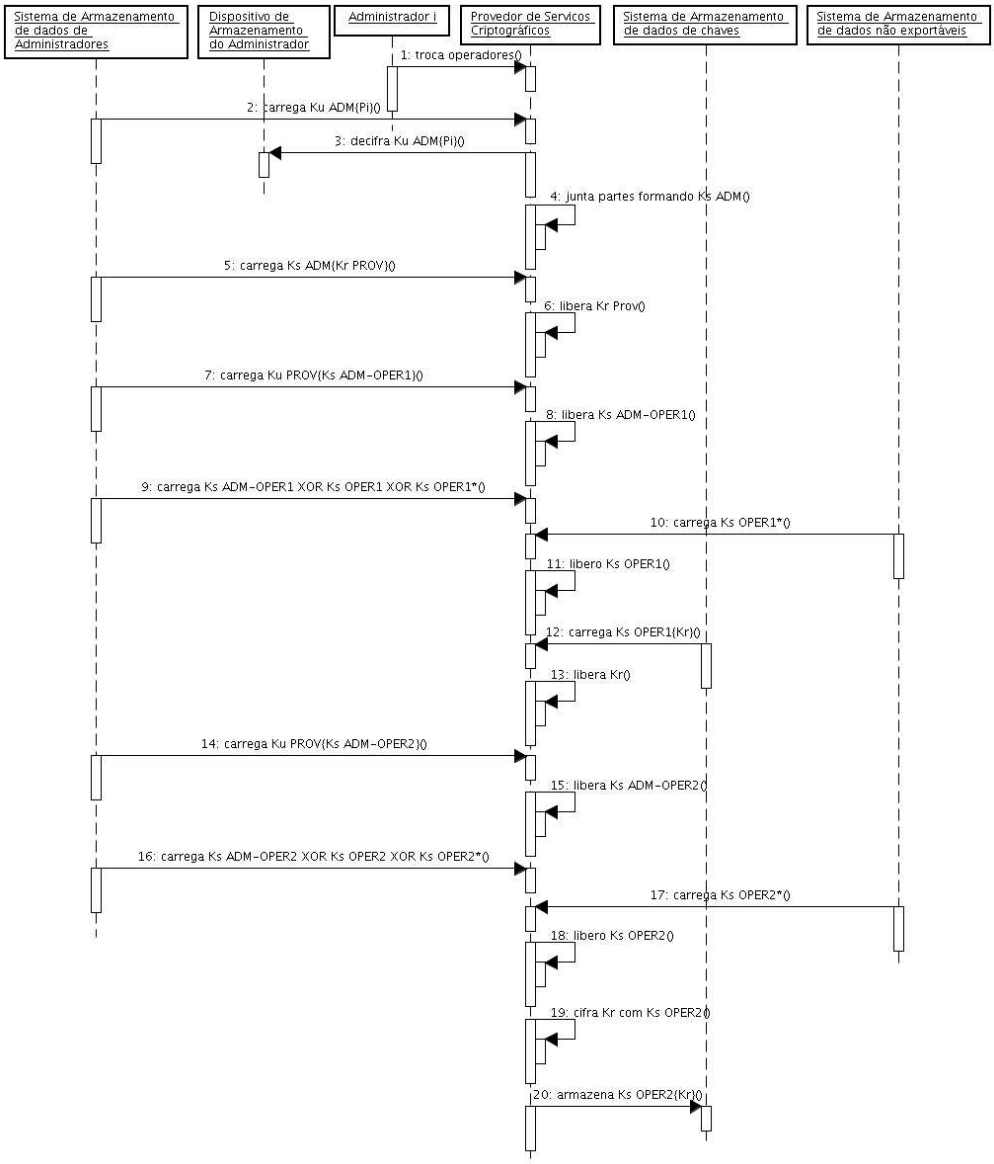

Figura 2.6: Mecanismos para troca de Operadores para uma Chave Assimétrica

Os passos do processo de troca de operadores serão representados pelos mesmos números do diagrama de seqüência, contido na figura 2.6. A descrição é a seguinte:

1. a solicitação de troca do grupo de operadores é encaminhada ao Provedor de Serviços Criptográficos;

2. por se tratar de uma tarefa administrativa, é necessária a autenticação dos administradores, executando o processo de desafio apresentado no início do capítulo. Para cada administrador é carregado do sistema de dados de administradores a parte do segredo cifrada;

3. a parte do segredo é decifrada pela chave privada, contida no dispositivo de armazenamento do administrador;

4. com todas as n partes, o Ks_{ADM} pode ser remontado pelo algoritmo de segredo compartilhado;

5. do sistema de dados de administradores é carregada a chave privada do PSC cifrado;

6. é permitida a decifragem de Kr_{PROV}, utilizando Ks_{ADM};

7. busca no sistema de armazenamento de dados de administradores a chave que liga o conjunto de administradores e o conjunto de operadores detentores atuais da chave. Esta chave está armazenada cifrada;

8. como já estamos de posse de Kr_{PROV}, é possível liberar $Ks_{ADM-OPER1}$;

9. busca no sistema de armazenamento de dados de administradores o resultado da operação lógica XOR;

10. carrega do sistema de dados não exportáveis o valor de Ks_{OPER1*};

11. com as chaves já carregadas é possível utilizar a característica de reversibilidade do XOR. Reaplica-se ao resultado do XOR, carregado no passo 9, as chaves $Ks_{ADM-OPER1}$ e Ks_{OPER1*}, reconstituindo o valor de Ks_{OPER1};

12. carrega do sistema de armazenamento de dados de chaves, a chave que se deseja trocar o grupo de operadores detentor;

13. de posse da chave assimétrica cifrada e da chave simétrica, pode-se decifrar Kr com Ks_{OPER1};

14. a partir desta operação, já com a chave assimétrica aberta, começa o processo de delegação ao novo conjunto de operadores. Inicia-se carregando a chave $Ks_{ADM-OPER2}$ cifrada que liga o conjunto de operadores com o conjunto de administradores;

15. decifra $Ks_{ADM-OPER2}$ com Kr_{PROV};

16. busca no sistema de armazenamento de dados de administradores o resultado da operação lógica XOR;

17. carrega do sistema de dados não exportáveis o valor de Ks_{OPER2*};

18. com as chaves já carregadas é possível utilizar a característica de reversibilidade do XOR. Reaplica-se ao resultado do XOR, carregado no passo 16, as chaves $Ks_{ADM-OPER2}$ e Ks_{OPER2*}, reconstituindo o valor de Ks_{OPER2};

19. a chave assimétrica Kr é cifrada por Ks_{OPER2};

20. a chave cifrada é armazenada no sistema de armazenamento de dados de chaves e finaliza o processo de troca do conjunto de operadores.

O ponto importante nesse processo está centrado no sistema de armazenando de dados Não Exportáveis. As chaves Ks_{OPER1*} e KS_{OPER2*} não são exportadas na realização da cópia de segurança do PSC. Essa exclusão garante que, caso seja recuperada a cópia de segurança em outro PSC, os administradores não consiguirão alterar o poder dos operadores sobre as chaves.

Os operadores, juntamente com os administradores, só poderão ser manipulados novamente após recomporem Ks_{OPER*}, utilizando o resultado do XOR, $Ks_{ADM-OPER}$ e Ks_{OPER}. Esse sistema garante a rastreabilidade das chaves.

2.7 Sistema para Cópia de Segurança

As cópias de segurança servem para manter em local e de forma segura os dados do Provedor de Serviços Criptográficos, possibilitando a continuidade do processo de uso mesmo em caso de desastre.

Este mecanismo é uma tarefa administrativa, necessitando a autenticação de n administradores. Ao solicitar ao PSC o início do processo, deve ser informado o valor de l, que será o número mínimo de administradores necessário para recuperar o segredo em outro PSC.

O valor de l deve seguir a seguinte fórmula: $1 \leq n \leq l \leq m$, respeitando que $m-l < n$, viabilizando a restrição de não existir duas instâncias do mesmo PSC rodando paralelamente. O processo de recuperação da cópia de segurança obriga a troca do conjunto de administradores, bem como a destruição dos administradores antigos.

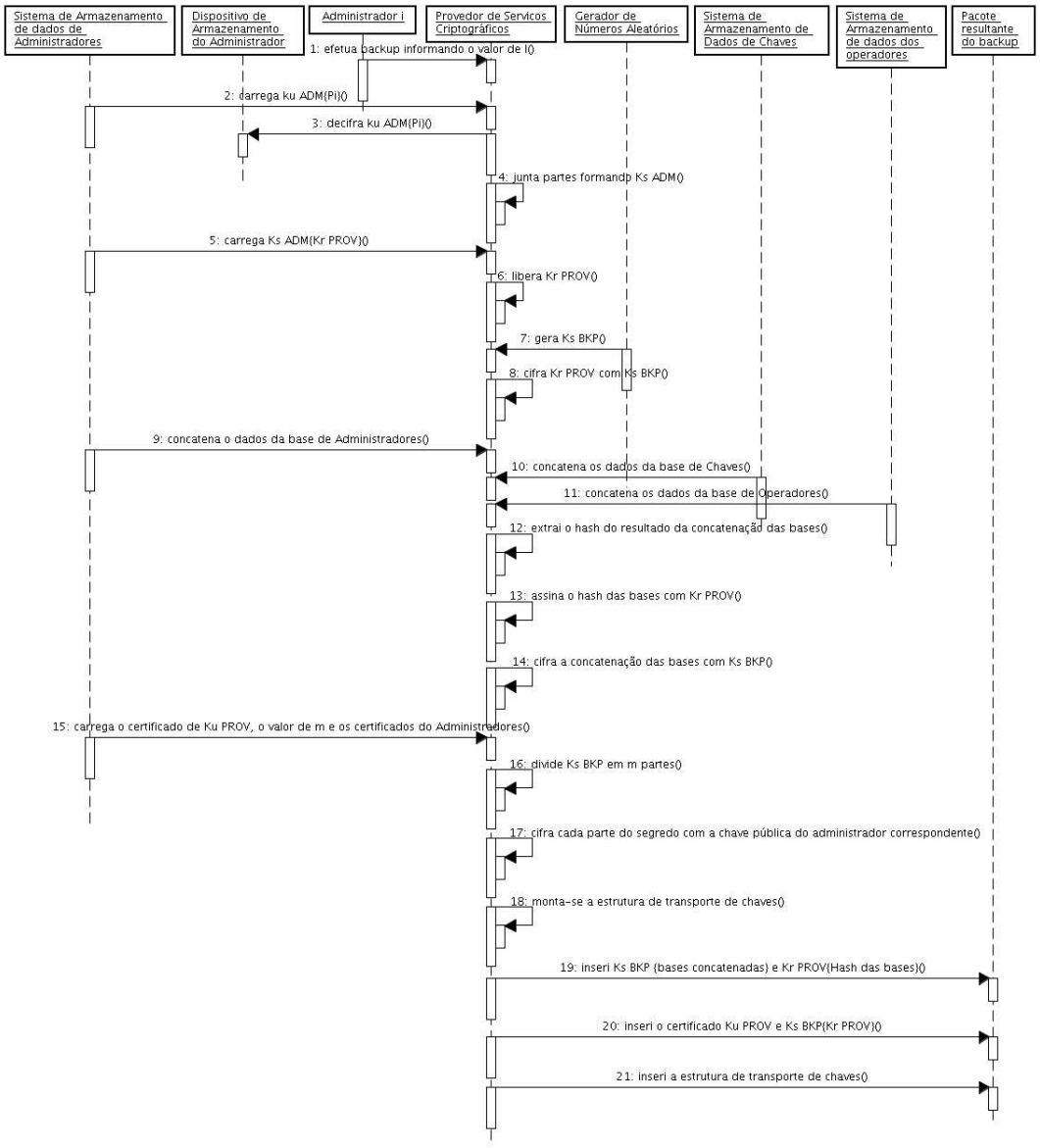

Figura 2.7: Mecanismos para realização da Cópia de Segurança

A figura 2.7 apresenta o mecanismo de execução da cópia de segurança.

Os passos são descritos a seguir:

1. a solicitação de cópia de segurança é encaminhada ao PSC, informando o valor de l, que será o número mínimo de administradores para recuperar a cópia;

2. por se tratar de uma tarefa administrativa, é necessária a autenticação dos administradores, executando o processo de desafio apresentado no início do capítulo. Para cada administrador, a parte do segredo cifrado é carregada do sistema de dados de administradores;

3. a parte do segredo é decifrada pela chave privada, contida no dispositivo de armazenamento do administrador;

4. Ks_{ADM} pode ser remontada, pelo algoritmo de segredo compartilhado, com todas as n partes do segredo;

5. a chave privada cifrada do PSC é carregada do sistema de dados de administradores;

6. é permitida a decifragem de Kr_{PROV} utilizando Ks_{ADM};

7. o Gerador de Números aleatório gera a chave Ks_{BKP};

8. a chave privada do PSC, Kr_{PROV}, é cifrada com Ks_{BKP};

9. as informações contidas no sistema de dados de administradores são armazenadas no pacote dos dados, o qual será posteriormente copiado;

10. adiciona ao pacote de dados da cópia, a base de dados de chaves;

11. adiciona ao pacote de dados da cópia, a base de dados de operadores;

12. com o pacote de dados, para a cópia, completo, aplica-se uma função de resumo, obtendo o hash do pacote;

13. o hash do pacote de dados é assinado por Kr_{PROV}, garantindo sua integridade;

14. o pacote de dados é cifrado por Ks_{BKP};

15. carrega o certificado do PSC, o valor de m e os certificados dos atuais administradores da base de dados de administradores;

16. divide, o segredo Ks_{BKP} em m partes;

17. utilizando os certificados dos administradores carregados no passo 15, cada parte é cifrada com o certificado correspondente.

18. com as partes cifradas e os dados de administradores, monta-se a estrutura de transporte de chaves;

19. insere no pacote final da cópia de segurança as bases de dados cifradas por Ks_{BKP} e o hash das bases de dados assinado, respectivamente realizadas nos passos 14 e 12;

20. adiciona no pacote final da cópia o certificado auto-assinado e a chave privada cifrada do PSC, respectivamente Ku_{PROV} e $Ks_{BKP}Kr_{PROV}$;

21. por fim, inclui a estrutura de transporte de chaves ao pacote final.

Ao final do processo, o ambiente interno ao PSC está copiado, sendo possível a recomposição em outro PSC. Este processo garante a autenticidade, integridade e segurança para posterior recuperação.

2.8 Recuperação de Cópia de Segurança

A recuperação da cópia de segurança visa a reconstrução de todo ambiente operacional de gerenciamento de chaves de um provedor já existente, seguindo todos os requisitos do processo.

Este processo é uma tarefa administrativa, que prevê a autenticação de l administradores. O valor de l foi informando no momento da realização da cópia de segurança. A figura 2.8 apresenta os passos deste processo. A descrição de cada um é apresentada a seguir:

1. a chamada do processo de recuperação da cópia de segurança é encaminhada ao PSC, informando o valor de n e m. Estes valores serão respectivamente o subconjunto mínimo para remontagem do segredo e o número total do novo conjunto de administradores;

2. a estrutura de transporte de chaves e a chave privada do PSC são carregadas do pacote final da cópia de segurança;

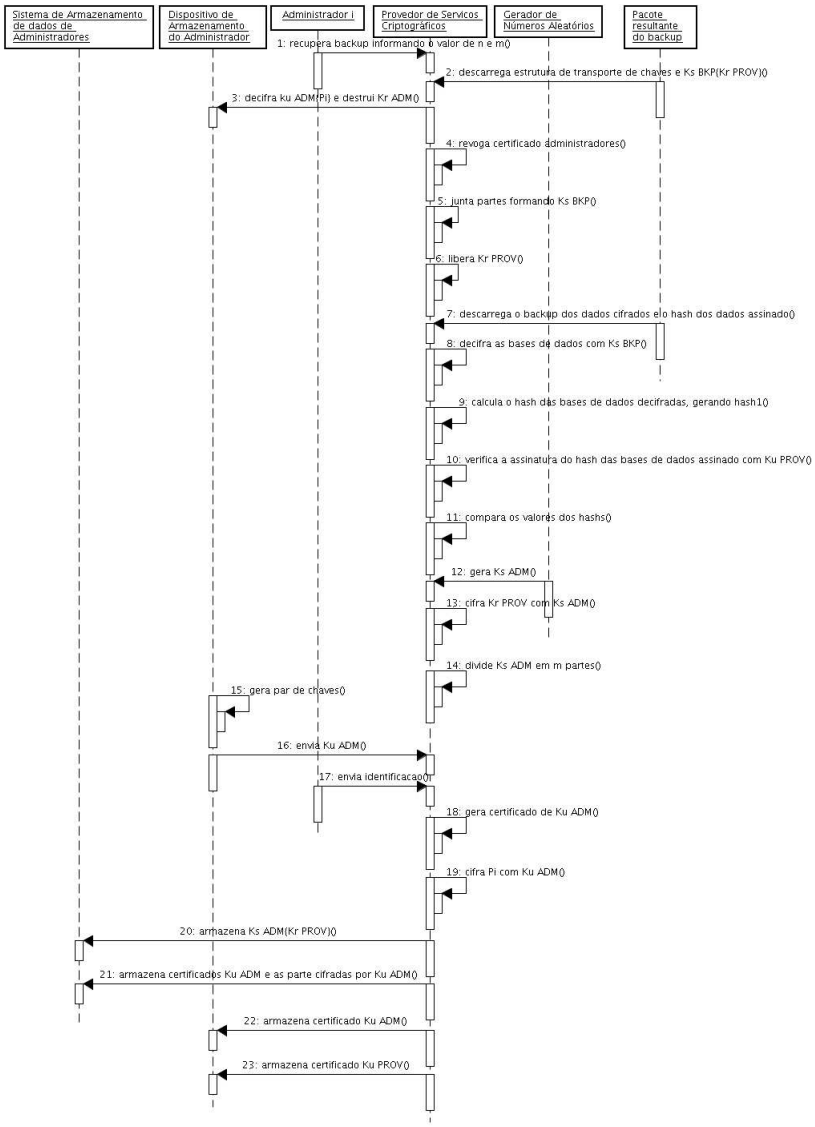

Figura 2.8: Mecanismos para recuperação da Cópia de Segurança

3. as partes do segredo, contidas na estrutura de transporte de chaves, são decifradas pela chave privada contida no dispositivo de armazenamento dos administradores, sendo destruídas logo após. A destruição é necessária para garantir que não exista duas instâncias do PSC operando em paralelo.

4. revoga os certificados de todo o conjunto de administradores do antigo PSC, impossibilitando seu uso;

5. com todas as partes do segredo decifrada, pode-se recuperar Ks_{BKP};

6. a chave privada do PSC, carregado no passo 2, é decifrada por Ks_{BKP}, possibilitando o seu uso;

7. retira do pacote final da cópia de segurança a cópia das bases de dados cifrados e o hash do mesmo, assinado;

8. as bases de dados são decifradas por Ks_{BKP}, recuperando os dados do sistema de dados de administradores, operadores e chaves;

9. calcula o hash das bases de dados decifradas, para posterior checagem de integridade no passo 11;

10. verifica a assinatura do hash das bases de dados extraídas do pacote final da cópia de segurança com Ku_{PROV};

11. os valores dos hashs obtidos no passo 9 e extraídos do pacote da cópia de segurança são comparados para checagem de integridade;

12. gera aleatoriamente o valor de Ks_{ADM}, que será a chave utilizada para cifrar a chave privada do PSC;

13. cifra Kr_{PROV}, com Ks_{ADM} gerada no passo anterior;

14. Ks_{ADM} é passado pelo algoritmo de compartilhamento de segredo, sendo dividido em m partes;

15. nos dispositivos de armazenamento dos administradores é gerado um par de chaves criptográficas, Kr_{ADM} e Ku_{ADM};

16. a chave pública dos administradores, ku_{ADM}, é extraída do dispositivo de armazenamento de cada um;

17. o administrador envia ao PSC suas informações de identificação para geração dos certificados;

18. os certificados para todos os administradores são gerados contendo as informações informadas anteriormente;

19. cada parte do segredo é cifrada com a chave pública de um administrador. Lembrando que são m partes do segredo e m administradores.

20. armazena a chave privada do PSC cifrada no sistema de armazenamento de dados dos administradores, $Ks_{ADM}Kr_{PROV}$;

21. no sistema de armazenamento de dados dos administradores, são inseridos os certificados dos administradores e as partes do segredo cifradas por eles.

22. importa o certificado de cada administrador para o seu dispositivo de armazenamento de administrador;

23. insere no dispositivo de armazenamento de administrador o certificado do PSC, Ku_{PROV};

Realizado o processo com sucesso, o PSC reconstruído possuirá novo conjunto de administradores, e a instância antiga do provedor não poderá mais ser operacionalizada. A destruição dos antigos administradores garante essa característica.

O novo PSC não contém os dados do sistema de armazenamento de dados não exportados, garantindo o requisito de rastreabilidade das chaves. A chave Ks_{OPER*} precisa ser reconstruída para cada grupo de operadores existente no provedor, necessitando a autenticação dos novos administradores e do próprio grupo de operadores em questão. Essa tarefa é viabilizada com a aplicação da operação lógica XOR, apresentada na seção 2.2.

2.9 O Conjunto de Auditores

O processo de criação do conjunto de auditores é tarefa necessária para operacionalização do Provedor de Serviços Criptográficos. O conjunto de auditores é um tipo especializado do conjunto de operadores. Os auditores têm o papel de fiscalizar os registros de utilização do PSC. Só eles têm o poder de ver e apagar os passos do PSC.

Este processo é uma tarefa administrativa, necessitando que n administradores se identifiquem, possibilitando a recomposição do segredo e por conseguinte a liberação de Kr_{PROV}.

As diferenças da criação do conjunto de operadores para a criação do conjunto de auditores são as seguintes:

- a parte componente do XOR representada por Ks_{OPER*}, que aqui é identificada como Ks_{AUDIT*} não é armazenada, impossibilitando os administradores de efetuarem qualquer mudança no conjunto de auditores sem a presença de k integrantes;

- junto com o conjunto de auditores, será criado um par de chaves assimétricas, que serão Kr_{AUDIT} e Ku_{AUDIT}. Será gerado um certificado de Ku_{AUDIT}. Todos os registros que o sistema gera serão cifrados com Ku_{AUDIT};

- para gerenciar os registros do sistema será necessária a autenticação dos auditores para recomposição de Ks_{AUDIT}, que na figura dos operadores é representada por Ks_{OPER};

- a chave privada dos auditores, Kr_{AUDIT} será armazenada cifrada por Ks_{AUDIT};

Este sistema de registro de eventos do PSC terá um tamanho limite, podendo os auditores examinar e limpar os dados contidos neste espaço a qualquer momento, perante autenticação. A lotação deste sistema implicará inoperância do provedor para quaisquer atividades, excluindo a possibilidade de limpeza desta área pelos auditores.

Capítulo 3

Definição da Aplicação e Problemas Enfrentados

O desenvolvimento da Aplicação Gestora de um Provedor de Serviços Criptográficos prevê definições inerentes ao domínio da solução, envolvendo a escolha da linguagem de desenvolvimento, a forma de execução e comunicação da aplicação e a descrição das bibliotecas utilizadas na implementação.

O final do capítulo contemplará os problemas enfrentados no desenvolvimento, abrangendo a falta de documentação das bibliotecas existentes no mercado e a inexistência de controle de execução dos Sistemas Operacionais.

3.1 Linguagem Adotada

A escolha da linguagem para desenvolvimento da aplicação seguiu os seguinte critérios:

- Desempenho;
- Otimização;
- Domínio Público;
- credibilidade comprovada;
- Ter portabilidade para os mais diversos sistemas operacionais;

- Ter bibliotecas livres com qualidade que implementem compartilhamento de segredo e técnicas conhecidas de criptografia;

- Rodar em plataforma com capacidade de processamento relativamente baixo.

Considerando os ítens anteriores, o desenvolvimento da aplicação foi feito, utilizando a linguagem C padrão, especificado pelo comitê do padrão ANSI.

A linguagem JAVA, que era uma segunda opção, foi preterida pelo fato da máquina virtual Java ocupar muito espaço e a capacidade de processamento necessária ser mais alta.

3.2 Comunicação e Forma de Execução da Aplicação Gestora

A aplicação gestora consistiu no desenvolvimento de duas aplicações: um cliente e um servidor.

O servidor, que estará embarcado no Módulo de Hardware Criptográfico, irá rodar automaticamente quando o provedor de serviços criptográficos for iniciado, sendo executado como um serviço do sistema operacional.

A comunicação será realizada pela interface de rede, padrão ethernet [21], escutando em uma porta do protocolo TCP [22]. Terá suporte para mais de uma conexão ao mesmo tempo, mas sempre lembrando que as funcionalidades são atômicas.

O cliente poderá ser executado antes de realizada a configuração inicial de qualquer máquina, com acesso via rede, ao PSC. O estabelecimento da conexão será cifrado, viabilizada através do protocolo SSL [23], tornando a escuta da rede por qualquer intruso ilegível. Após configurado o servidor, serão gerados pares de chaves com certificado emitido pela Autoridade Certificadora interna ao PSC, para todos os clientes previamente autorizados para estabelecimento da conexão. A autorização será feita para o endereço de rede dos clientes.

3.3 Dispositivo de Armazenamento de Usuários

Os mecanismos de gerenciamento de chaves criptográficas prevêem para cada usuário do Provedor de Serviços Criptográficos, um dispositivo para armazenamento das chaves privada, pública e certificados. Ele deve ser capaz de realizar, internamente, operações criptográficas, não tendo que expor a chave privada em nenhum momento.

Os dispositivos escolhidos para o protótipo foram smartcards, por serem uma prática segura de identificação de usuários de um sistema. Pensando nisso, todas as autenticações da Aplicação Gestora foram desenvolvidas utilizando-os.

Smartcard são dispositivos que implementam funções criptográficas em hardware, proporcionando maior segurança e pouca volatilidade. Em contra partida, de maneira geral, não existe como realizar backup. Foram especificados pela norma ISO/IEC 7816-4 [24], que definem características físicas, dimensões e requisitos mínimos de segurança.

Nos smartcards, existe um sistema operacional para processamentos criptográficos e controle de acesso. O armazenamento de chaves é através de um sistema de arquivos especificado pelo padrão PKCS#15 [25], com diretórios, arquivos e controle de permissões (criação, leitura, escrita).

A utilização dos smartcards é viabilizada por dois componentes de hardware: os leitores e os smartcards. Os requisitos de software são: uma aplicação que através dos drivers do leitor consiga trocar informações com os smartcards, e uma aplicação que contenha os drivers do modelo do smartcard e consiga trocar informações com o mesmo.

A versão dos smartcards utilizados foi a SPK 2.3, da empresa G&D Burti, a qual tem capacidade de armazenamento de 32Kb e suportam chaves de até 1024 bits.

Os leitores escolhidos foram os modelos towitoko, da empresa CHIP-DRIVE , que são interligados ao computador pela porta USB. Os critérios de seleção foram a compatibilidade com as bibliotecas já existentes e os custos para acesso a tecnologia.

3.4 Bibliotecas Utilizadas

Para o desenvolvimento da aplicação com os mecanismos de gerenciamento já citados, controles de segurança e gerenciamento da aplicação, optou-se por utilizar as seguintes bibliotecas:

- POSIX Thread;
- OpenCT;
- OpenSC;
- SQLite;
- Share Secret;
- OpenSSL.

O grande motivo pela opção destas bibliotecas foi por serem livres e implementadas na linguagem escolhida para desenvolvimento, C. A implementação de todas as funcionalidades necessárias para a Aplicação gestora foi descartada por despender muito tempo e já existirem, no mercado, bibliotecas para esse fim, com qualidade comprovada.

A descrição de cada biblioteca é apresentada a seguir.

3.4.1 POSIX Thread

Uma thread é definida como um fluxo de execução independente de um conjunto de instruções. Este recurso é utilizado para gerenciar as várias conexões que por ventura sejam solicitadas à aplicação servidor.

Especificada pelo padrão IEEE POSIX 1003.1c [26], a Pthread, como também é conhecida, foi implementada pela falta de compatibilidade entre as várias implementações de thread existentes no mercado. Cada fabricante que desejasse esse recurso, utilizava sua própria biblioteca.

A biblioteca Pthread foi implementada em C, facilitando a utilização no PSC. Outro ponto forte é sua performance, ela apresenta desempenho superior ao da outra técnica conhecida, fork.

3.4.2 OpenCT

O uso de smartcard para autenticar os usuários do Provedor de Serviços Criptográficos, PSC, cria um requisito funcional de uso de leitores para os mesmos.

A biblioteca OpenCT [27] é uma API de código livre desenvolvida para detectar e utilizar os leitores de smartcard. Ela realiza toda a troca de mensagens entre a API que gerencia o smartcard e o smartcard propriamente dito.

3.4.3 OpenSC

OpenSC [28] é uma biblioteca com ferramentas e API para gerenciamento de smartcards, recurso utilizado para autenticar usuários. Trabalha em uma camada de mais alto nível, isto é, abstrai a forma de comunicação com o leitor e com o próprio smartcard.

Este conjunto de ferramentas trabalha integrado com a API apresentada anteriormente, trabalhando de forma transparente.

3.4.4 SQLite

Qualquer sistema desenvolvido precisa de uma forma para armazenar informações, e esse projeto não é diferente. Apesar de não serem muitos dados, o desenvolvimento de um sistema de armazenamento específico seria necessário se não existisse uma ferramenta capaz de cumprir os requisitos necessários.

SQLite [29] é um sistema de banco de dados simples de administrar, operar, embarcar e customizar. É operacionalizado através de linguagem SQL [30].

Apesar do tamanho e da rapidez proporcionada, tem bastante recursos e confiabilidade. Um sistema de dados completo é armazenado em apenas um arquivo, ajudando a organização.

3.4.5 Share Secret

O uso de segredo compartilhado é componente dos mecanismos de gerenciamento apresentados anteriormente. A implementação de uma biblioteca deste tipo despenderia muito tempo e seria trabalho dobrado, por já existir uma biblioteca de código aberto capaz de fazer o que o sistema propôs.

A implementação da biblioteca Sharesecret [31] foi realizada por não existir no mercado ferramenta semelhante, trazendo ao mundo do software livre uma implementação prática e funcional.

3.4.6 OpenSSL

O projeto OpenSSL [32] é um esforço colaborativo para desenvolver um conjunto de ferramentas de nível comercial, robusto e completo. O OpenSSL implemeta os protocolos de camada de soquetes seguros (SSL) e camada de transporte seguro (TLS) além de uma biblioteca completa de criptografia, gerenciada por uma comunidade mundial de voluntários que usam a internet para se comunicar, planejar e desenvolver o conjunto de ferramentas OpenSSL e a documentação relacionada.

O conjunto de ferramentas possui uma ferramenta de linha de comando muito rica de recursos, uma API que implementa os protocolos SSL e TLS e, também, uma API com todos os recursos de criptografia utilizados como padrão na Internet.

A confiança nesta biblioteca aumenta ao saber que o OpenSSH [33] e o OpenPGP [34] foram desenvolvidos utilizando-a. É, sem sombra de dúvida, o conjunto de ferramentas criptográficas mais completo, confiável e conhecido.

3.5 Ambiente de Desenvolvimento

O Ambiente de desenvolvimento escolhido para implementação da aplicação proposta foi o Eclipse.

O Eclipse [35] é uma plataforma aberta para prover integração de ferramentas de desenvolvimento, inicialmente proposto para implementações na linguagem JAVA. Esta plataforma contém extensões passíveis de integração, permitindo implementação de programas em linguagem C, uso de controle de versão e sistema de documentação, concentrados em um único ambiente.

A praticidade foi a característica relevante para a escolha da IDE.

3.6 Sistema de Documentação

A documentação de qualquer aplicação é um ponto muito importante para o sucesso de um projeto. Pensando nisso, e sabendo que a documentação, apesar de importante, é a primeira coisa a ser deixada de lado com o aperto do prazo, foi escolhido um sistema de documentação prático e simples de ser realizado e com vários formatos de saídas configuráveis.

A praticidade foi adquirida com o uso de um sistema de documentação, realizado diretamente no código fonte da aplicação. Esta forma também possibilitou maior fidelidade da documentação. É simples, sua sintaxe no código é semelhante a um trecho de comentário.

As saídas do sistema podem ser em HTML, LATEX, PDF e páginas de manuais UNIX. Estas escolhas foram incentivadas por abrangerem todas as possibilidades de utilização.

Seguindo todos os pontos citados acima, e também por existir um módulo capaz de se integrar ao ambiente de desenvolvimento descrito acima (eclipse), foi escolhido o sistema de documentação Doxygen.

Doxygen [36] é um sistema de documentação utilizado para muitas linguagens e integrado a grande maioria de ambientes de desenvolvimento. Extrai diretamente do código fonte a documentação e monta a saída final, em segundos, sem intervenção do programador.

3.7 Problemas Enfrentados

3.7.1 Documentação das Bibliotecas Utilizadas

A implementação do Provedor de Serviços Criptográficos, PSC, foi viabilizada com a utilização de várias bibliotecas existentes no mercado. Para o uso das mesmas é preciso ter pleno conhecimento do funcionamento da API.

A documentação vem como a mais importante forma de conhecimento de bibliotecas e é nesse ponto que ocorre o grande problema, praticamente não existe documentação.

Os desenvolvedores implementam bibliotecas muito boas e úteis, mas

com pouca ou nenhuma documentação, obrigando a leitura do código fonte para uso das mesmas no desenvolvimento de outras aplicações.

3.7.2 Controle de Execução de Programas

A linguagem C é uma linguagem de baixo nível, precisando de um controle rigoroso na implementação, para que não ocorram problemas na execução. Seu compilador não realiza controle de tamanho de buffer, ficando a cargo do programador seu controle.

Considerando que o desenvolvimento foi realizado em uma distribuição linux, a execução que parecia estar perfeita, ao ser portada para OpenBSD, sistema que roda o PSC, apresentou vários problemas. Entre eles, o controle rigoroso de estouro de buffer, isto é, o uso de mais memória do que foi previamente alocado é detectado pelo sistema operacional.

O sistema operacional OpenBSD se mostrou mais confiável em termos de execução de programas desenvolvidos em C, aumentando consideravelmente a segurança da execução.

Capítulo 4

Aplicação Gestora Desenvolvida

A aplicação gestora abrangeu o desenvolvimento de duas aplicações, o cliente e o servidor, sendo que o servidor irá rodar no interior do Provedor de Serviços Criptográficos.

Os detalhes do desenvolvimento serão divididos da mesma forma que os mecanismos de gerenciamento, com descrição de cada um deles.

Algumas das atividades utilizadas em praticamente todos os mecanismos terão seções separadas, como sistema de armazenamento e iterações com smartcards.

4.1 Iterações com Smartcards

O uso de smartcards é uma prática segura de identificação de usuários de um sistema. Pensando nisso, todas as autenticações da Aplicação Gestora foram desenvolvidas, utilizando-os. Mas antes vamos entender como funciona um smartcard.

O OpenCT será a aplicação de mais baixo nível, que terá o driver do leitor e trocará informações com o mesmo. O OpenSC será o componente que trocará informações diretamente com os cartões STARCOS SPK 2.3, abstraindo a questão do leitor. Estas aplicações são desenvolvidas no mesmo projeto, tendo integração completa.

Um smartcard, quando sai de fábrica, vem com seu sistema de arquivo zerado, isto é, completamente formatado. A primeira e única coisa a fazer é a criação de PIN (usuário) para o smartcard. Esta criação resume-se à especificação de uma senha para acesso a este usuário. Essa senha gravada é o chamado PIN.

A criação de um PIN é que possibilita a criação de chaves vinculadas.

Todas as chaves criadas no smartcard têm um identificador único. Cada chave privada pode ter uma chave pública e um certificado com o mesmo identificador, caracterizando a ligação entre os três objetos.

A chave privada criada em um smartcard não pode ser extraída em momento algum, por restrições de especificações do padrão. As operações de assinatura e decifragem, utilizando a chave privada, são solicitadas ao smartcard e realizada internamente. As chaves públicas e os certificados podem ser extraídos.

O OpenSC disponibiliza três aplicações para gerenciar smartcards: uma para criação de PINs e pares de chaves nos smartcards; uma para exploração do conteúdo e extração de chaves públicas e certificados; e outra para utilização das chaves privadas contidas nos smartcards.

O principal processo de autenticação, utilizando smartcards, é o protocolo do desafio. O protocolo consiste dos seguintes passos:

1. gera-se um número randômico;
2. é cifrado esse número com a chave pública do usuário (a chave pública está contida no certificado referente à chave privada);
3. o número cifrado é decifrado, utilizando a chave privada, que só existe no interior do smartcard
4. realiza-se a checagem de igualdade entre o número inicial gerado com o resultado da decifragem. Se a igualdade for positiva, o usuário é autenticado.

4.2 Sistema de Armazenamento

O armazenamento foi realizado em várias tabelas de várias bases de dados, separadas por categorias.

4.2.1 Administradores

Esta categoria engloba todos os dados considerados administrativos, tais como parte dos segredos capazes de liberar uma chave, $Ks_{ADM-OPER}$, dados dos administradores.

Foram definidas três tabelas, uma com os dados gerais dos administradores, outra com informações específicas e outra com informações administrativas de chaves.

Tabela de Dados Gerais dos Administradores

Esta tabela apresenta as seguintes colunas:

- cd_hsm - código identificador da tabela, é uma chave primária.
- m - número de administradores definidos na criação.
- n - número mínimo de administradores necessários para autenticação.
- crypt_key - nome do arquivo onde está armazenada a chave privada do PSC.
- cert_file - nome do arquivo onde está o certificado referente à chave privada do PSC.
- id_used - valor que informa qual é a configuração válida. Nesta tabela, deve existir, no máximo, uma linha valendo 1 (um). Isto deve-se a tentativas frustadas de criação do grupo de administradores, ou várias trocas de administradores, ficando um histórico das tentativas.

Cada linha desta tabela representa um grupo de administradores, na qual, todos os campos são obrigatórios e a coluna id_used pode assumir os valores de 1 (um) ou 0 (zero). O grupo de administradores válidos é o que tiver valor 1 (um) para este campo.

Tabela de Dados Específicos dos Administradores

Esta tabela apresenta as seguintes colunas:

- cd_adm - código identificador da tabela, é uma chave primária.
- adm_num - número do administrador na seqüência de criação. Varia de 1 (um) a m.
- user_pin - número de PIN informado pelo administrador. Lembrando que o número de PIN informado não é o mesmo utilizado para acessar o smartcard.

- auth_id - número identificador do administrador no smartcard. No smartcard, o identificador é único para cada PIN.
- pin - número do PIN utilizado para acessar o smartcard. Número de 8 (oito) dígitos gerado randomicamente.
- puk - número do PUK gravado no smartcard. Esse número é utilizado em caso de perda do PIN ou no caso de errar três vezes o PIN. Número de 8 (oito) dígitos gerado randomicamente.
- key_id - número identificador da chave privada no smartcard. Para utilizar a chave privada de um administrador é preciso saber seu identificador.
- cert_id - número identificador do certificado no smartcard. Para utilizar o certificado de um administrador é preciso saber seu identificador.
- crypt_part - nome do arquivo que contém a parte do segredo compartilhado cifrado.
- cd_hsm - código identificador do grupo de administradores ao qual este administrador pertence. Cada configuração terá m administradores se completada com sucesso. Cada linha desta tabela representa um administrador, onde todos os campos são obrigatórios. O campo cd_hsm representa o grupo ao qual um administrador pertence.

Tabela de Dados Administrativo de Chaves

Esta tabela apresenta as seguintes colunas:

- cd_admoper - código identificador da tabela, é uma chave primária.
- cd_goper - código identificador do grupo de operadores ao qual a chave pertence. Restringe esse valor apenas a grupos de operadores existentes e válidos.
- xor_ks - valor final do xor (ou exclusivo) realizado sobre as chaves simétricas do grupo de operadores, dos administradores e da chave não exportável.
- crypt_ksadmoper - nome do arquivo que contém o conteúdo de ks_admoper cifrado.

Cada linha desta tabela representa uma chave existente no PSC. Ela é povoada no momento da criação do par de chaves.

4.2.2 Operadores

Esta categoria engloba os dados dos grupos de operadores e os operadores integrantes destes grupos.

Tabela de Dados de Grupo de Operadores

Esta tabela apresenta as seguintes colunas:

- cd_goper - código identificador da tabela, é uma chave primária.
- l - número de operadores definidos na criação.
- k - número mínimo de operadores necessários para autenticação.
- nm_goper - nome identificador do grupo de operadores. Cada grupo é identificado por um nome único.
- id_used - valor que informa se a linha é um grupo de operadores válido. O uso desta coluna é importante porque no início do processo de criação do grupo de operadores é gerada essa linha com esta coluna com valor 0 (zero) e a execução pode ser abortada por algum motivo, não tornando válida esta configuração. No final do processo, se tudo ocorrer como esperado, é alterado esse campo para 1 (um).

Cada linha desta tabela representa um grupo de operadores válido ou não, fazendo valer o valor do campo id_used. Se este campo tiver valor 1 (um), este grupo é válido.

Tabela de Dados de Operadores

Esta tabela apresenta as seguintes colunas:

- cd_oper - código identificador da tabela, é uma chave primária.
- oper_num - número do operador na seqüência de criação. Varia de 1 (um) a m.
- user_pin - número de PIN informado pelo operador. Lembrando que o número de PIN informado não é o mesmo utilizado para acessar o smartcard.

- auth_id - número identificador do operador no smartcard. No smartcard, o identificador é único para cada PIN.

- pin - número do PIN utilizado para acessar o smartcard. Número de 8 (oito) dígitos gerado randomicamente.

- puk - número do PUK gravado no smartcard. Esse número é utilizado em caso de perda do PIN ou no caso de errar três vezes o PIN. Número de 8 (oito) dígitos gerado randomicamente.

- key_id - número identificador da chave privada no smartcard. Para utilizar a chave privada de um operador é preciso saber seu identificador.

- cert_id - número identificador do certificado no smartcard. Para utilizar o certificado de um operador é preciso saber seu identificador.

- crypt_part - nome do arquivo que contém a parte do segredo compartilhado cifrado.

- common_name - nome do operador informado na criação do seu certificado.

- cd_goper - código identificador do grupo de operadores ao qual este operador pertence. Cada grupo terá l operadores.

Cada linha desta tabela representa um operador que é participante do grupo representado pelo código cd_goper. Todos os campos são obrigatórios e o grupo de operadores deve ser válido para utilização de um operador.

4.2.3 Chaves

Essa categoria engloba apenas dados das chaves gerenciadas pelo Provedor de Serviços Criptográficos. Ela é capaz de informar a que grupo de operadores pertence cada chave.

Tabela de Dados de Chaves

Esta tabela apresenta as seguintes colunas:

- cd_key - código identificador da tabela, é uma chave primária.

- nm_key - nome identificador do par de chaves gerenciado pelo Provedor de Serviços Criptográficos. Cada chave é identificado por um nome único.
- nm_prvkey - nome do arquivo que contém a chave privada.
- nm_pubkey - nome do arquivo que contém a chave pública.
- cd_goper - código identificador do grupo de operadores que detém o poder de uso da chave.

Cada linha desta tabela representa um par de chaves gerenciadas pelo Provedor de Serviços Criptográficos. Todos os campos são obrigatórios e, como restrição, o código identificador do grupo de operadores deve ser um código válido, isto é, existir e ter o campo id_used setado para 1 (um).

4.2.4 Dados Não Exportáveis

Esta categoria engloba os dados que não serão exportados na execução das rotinas de backup para garantir a rastreabilidade das chaves.

Tabela de Dados Não Exportáveis

Esta tabela apresenta as seguintes colunas:

- cd_notexport - código identificador da tabela, é uma chave primária.
- ks_operstart - chave simétrica gerada aleatoriamente que será componente ou exclusivo na recuperação do segredo do operador.
- cd_goper - código identificador do grupo de operadores correspondente a essa chave simétrica.

4.2.5 Cópia de Segurança

Essa categoria engloba apenas dados do processo de realização da cópia de segurança. Por se tratar de uma tarefa administrativa, os dados aqui contidos são de administradores.

Tabela de Dados Gerais da Cópia de Segurança

Esta tabela apresenta as seguintes colunas:

- cd_bkp - código identificador da tabela, é uma chave primária.
- l - número mínimo de administradores necessários para recuperação da cópia de segurança.
- m - número total de administradores. Este campo é buscado das tabelas de administradores.
- cipher_key - nome do arquivo onde está armazenada a chave privada do PSC. Cifrada com Ks BKP.
- cert_file - nome do arquivo onde está o certificado referente à chave privada do PSC.
- id_used - valor que informa qual é a configuração de cópia de segurança válida. Nessa tabela, deve existir, no máximo, uma linha valendo 1 (um). Isso deve-se a tentativas frustradas de execução de cópias de segurança, ficando um histórico das tentativas.

Esta tabela é semelhante a tabela de dados gerais de administradores. A diferença está no número mínimo de administradores necessário para a recuperação da cópia da chave simétrica que cifra a chave privada do PSC. Todos os campos são obrigatórios. A configuração de backup válida para a posterior recuperação é a linha setada como 1 (um) o campo id_used.

Tabela de Dados Específicos da Cópia de Segurança

Esta tabela apresenta as seguintes colunas:

- cd_bkpusers - código identificador da tabela, é uma chave primária.
- bkp_num - número do administrador na seqüência de criação. Varia de 1 (um) a m.
- auth_id - número identificador do administrador no smartcard. No smartcard, o identificador é único para cada PIN.

- xor_pins - ou exclusivo entre o PIN do smartcard com o PIN informado pelo usuário. Dessa forma, o PIN do smartcard pode ser recuperado facilmente se os dados que o usuário informar estiverem correto.

- key_id - número identificador da chave privada no smartcard. Para utilizar a chave privada de um administrador é preciso saber seu identificador.

- cert_id - número identificador do certificado no smartcard. Para utilizar o certificado de um administrador é preciso saber seu identificador.

- nm_cert_file - nome do arquivo que contém a parte do segredo compartilhado cifrado.

- nm_cipher_part - nome do arquivo que contém a parte do segredo compartilhado cifrado.

- cd_bkp - código identificador da configuração de cópia de segurança a qual pertence o administrador. Cada configuração terá m administradores se for completada com sucesso.

Cada linha desta tabela representa um administrador participante do processo de cópia de segurança, onde todos os campos são obrigatórios. O campo cd_bkp representa a configuração de cópia de segurança a qual o administrador pertence.

Tabela de Dados Temporário da Cópia de Segurança

Esta tabela apresenta as seguintes colunas:

- cd_tempbkp - código identificador da tabela, é uma chave primária.

- auth_id - número identificador do administrador no smartcard. No smartcard o identificador é único para cada PIN.

- new_pin - novo número do PIN utilizado para acessar o smartcard. Número de 8 (oito) dígitos gerado randomicamente.

- user_pin - número de PIN informado pelo administrador. Lembrando que o número de PIN informado não é o mesmo utilizado para acessar o smartcard.

- old_pin - antigo número do PIN utilizado para acessar o smartcard. Número de 8 (oito) dígitos gerado randomicamente.

Esta é uma tabela temporária, utilizada apenas no processo de recuperação da cópia de segurança. Para evitar a existência de duas instâncias do Provedor de Serviços Criptográficos, o PIN dos smartcards dos administradores antigos são alterados após sua autenticação. Mas isso pode gerar uma falha se o processo de recuperação der algum problema no meio da sua realização. Por isso, são guardados os dados dos administradores autenticados e seus PINs antigos recuperados para manter a antiga instância funcional.

Todos os campos são obrigatórios. Sempre, depois de recuperado ou não a cópia de segurança, esta tabela é limpa.

4.2.6 Configurações

Essa categoria engloba dados da configuração do Provedor de Serviços Criptográficos. Tem dados das chaves, da rede e dos certificados da Aplicação Gestora.

Tabela de Configurações de Certificados

Esta tabela apresenta as seguintes colunas:

- cd_cert - código identificador da tabela, é uma chave primária.
- nsComent - campo de comentário na geração de certificados.
- countryName - nome do País onde o PSC está instalado
- stateOrProvinceName - nome do estado onde o PSC está instalado
- localityName - nome da cidade onde o PSC está instalado
- organizationName - nome da organização onde o PSC está instalado
- organizationalUnitName - nome da unidade da organização onde o PSC está instalado
- commonName - nome utilizado no certificado auto-assinado interno do PSC
- expireHSM - tempo de validade do certificado da chave privada interna do PSC

- expireAdm - tempo de validade dos certificados dos administradores
- expireOper - tempo de validade dos certificados dos operadores
- expireSSL - tempo de validade do certificado criado para a conexão SSL.
- serial - número de série de emissão de certificados da Entidade Certificadora interna ao PSC. A cada certificado tem seu número único. Cada emissão de certificado esse número é incrementado
- id_used - valor que informa qual é a configuração de certificados válida. Nessa tabela, deve existir, no máximo uma linha com valor 1 (um). Isso deve-se a tentativas frustradas de execução de configuração, ficando um histórico das tentativas.

Os campos aqui contidos serão utilizados na geração de certificados na Entidade Certificadora interna ao PSC. Todos os campos são obrigatórios.

Tabela de Configurações de Chaves

Esta tabela apresenta as seguintes colunas:

- cd_keys - código identificador da tabela, é uma chave primária.
- cipher - nome identificador do algoritmo simétrico utilizado para armazenar as chaves privadas cifradas.
- usage_keys_length - tamanho das chaves gerenciadas pelo PSC
- hsm_keys_length - tamanho da chave do PSC
- adm_keys_length - tamanho das chaves dos administradores
- oper_keys_length - tamanho das chaves dos operadores
- id_used - valor que informa qual é a configuração de chaves válida. Nessa tabela, deve existir, no máximo, uma linha com valor 1 (um). Isso deve-se a tentativas frustradas de execução de configuração, ficando um histórico das tentativas.

Existem restrições para tamanho de chaves dos administradores e operadores porque os smartcards que serão usados para autenticá-los só permitem chaves de 1024 bits. Todos os campos são obrigatórios.

Tabela de Configurações de Rede

Esta tabela apresenta as seguintes colunas:

- cd_net - código identificador da tabela, é uma chave primária.
- hsm_ipaddr - endereço IP que o PSC irá operar
- hsm_netmask - máscara de rede que o PSC irá operar
- hsm_port - porta TCP que o PSC irá escutar para receber novas conexões
- client_ipaddr - endereço IP do cliente que irá acessar o PSC. Esse campo é importante para a configuração interna do firewall no PSC.
- id_used - valor que informa qual é a configuração de rede válida. Nessa tabela, deve existir, no máximo, uma linha com valor 1 (um). Isso deve-se a tentativas frustradas de execução de configuração, ficando um histórico das tentativas.

A configuração desta tabela deve ser feita com bastante cuidado. O PSC está configurado para buscar as informações de execução nesta tabela, possibilitando a configuração de um firewall dinâmico, aumentando a segurança. Somente conexões vindas do endereço IP informado para cliente serão aceitas. Todos os campos são obrigatórios.

4.3 Configuração do Provedor de Serviços Criptográficos

A partir deste ponto estão descritos os passos executados durante a manipulação do Provedor de Serviços Criptográficos, isto é, execução da Aplicação Gestora. Como primeiro e único passo possível, precisa-se configurar o PSC com a execução do comando hsm init.

Este processo basicamente pede para o usuário definir configurações de chaves, certificados e da rede onde o HSM irá operar. Se já existir uma configuração válida, a execução é abortada, retornando uma mensagem de erro ao cliente.

As configurações de chaves definidas nesta etapa são:

- método de cifragem simétrica utilizada para armazenar as chaves privadas. O padrão utilizado é AES de 256 bits, utilizando o método CBC.

- tamanho padrão para as chaves que serão gerenciadas pelo PSC, não querendo limitar os tamanhos de chaves. As chaves podem ser criadas de tamanho diferente se informado no momento da criação.

- tamanho da chave do PSC. Esta chave será equivalente a uma Entidade Certificadora, mas interna ao PSC. O padrão utilizado é 4096 bits.

- tamanho das chaves dos administradores do PSC. Esse tamanho tem que respeitar a capacidade de tamanho das chaves suportados pelos smartcards, normalmente 1024 bits.

- tamanho das chaves dos operadores do PSC. Também precisam respeitar o limite da capacidade de tamanho das chaves suportados pelos smartcards, normalmente 1024 bits.

Todas as configurações possuem configurações padrões, como foram citadas acima.

As configurações de certificados definidas nesta etapa são:

- descrição a ser inserida em todos os certificados gerados pelo PSC

- código do país onde o PSC irá operar. Informação incluída em todos os certificados emitidos pelo PSC

- estado ou província onde o PSC irá operar. Informação incluída em todos os certificados emitidos pelo PSC

- nome da organização detentora do PSC. Informação incluída em todos os certificados emitidos pelo PSC

- nome unidade da organização detentora do PSC. Informação incluída em todos os certificados emitidos pelo PSC

- nome do PSC, que será inserido no certificado da Entidade Certificadora interna. Para os certificados dos administradores e operadores será solicitado no momento de sua geração

- tempo de validade do certificado da Entidade Certificadora interna. Essa mensuração é feita em números de dias
- tempo de validade dos certificados dos administradores. Também mensurado em número de dias
- tempo de validade dos certificados dos operadores. Também mensurando em número de dias
- tempo de validade do certificado gerado para a utilização na conexão SSL após realizada a configuração

As configurações de rede definidas nesta etapa são:

- endereço IP que o PSC irá utilizar. O PSC possui uma configuração inicial, com o endereço 192.168.10.1
- máscara de rede que o PSC irá utilizar. A configuração inicial é 255.255.255.0
- número da porta na qual o servidor da Aplicação Gestora irá escutar novas conexões
- endereço IP da estação que irá rodar a aplicação cliente. Essa configuração é importante, pois somente conexões vindas deste endereço serão aceitas

Todos os grupos de configurações foram tratados internamente como estruturas de dados. As estruturas, depois de carregadas, são extraídos os dados para colocar no banco de dados. Os dados ficam então gravados para posterior uso. Se qualquer problema ocorrer durante a execução, a configuração não será validada, permanecendo as iniciais.

O Provedor de Serviços Criptográficos será reinicializado se a configuração ocorrer com sucesso. O PSC já irá inicializar com as configurações informadas.

4.4 Zerador do Provedor de Serviços Criptográficos

O Provedor de Serviços Criptográficos pode ser limpo, isto é, excluída todas as informações já geradas, tornando o PSC com as configurações de fábrica. Esta é uma tarefa administrativa, solicitando autenticação dos mesmos. Caso ainda não exista administradores válidos, a limpeza é executada diretamente.

Para zerar o PSC deve-se executar o comando hsm erase. Será solicitado confirmação para execução.

4.5 Criação de Administradores

A criação dos administradores do Provedor de Serviços Criptográficos é o próximo e único passo a ser realizado, após executada a configuração. O comando capaz de criá-los é adm genadm. Este comando necessita de alguns parâmetros.

Os parâmetros devem informar o número de administradores e quantidade mínima para recomposição do segredo, respectivamente m e n. Estes dois parâmetros são obrigatórios, sendo ignorados os que diferenciarem dos anteriores.

Após iniciada a execução, são realizadas duas checagens para determininação do estado interno do PSC, viabilizando a possibilidade de continuar. É checado se já existe uma configuração válida e também se não existe um grupo de administradores válidos. Estes são requisitos obrigatórios, abortando a execução e retornando uma mensagem de erro se não tiver sucesso.

O próximo passo é a geração do par de chaves interno do PSC. Um certificado auto-assinado é gerado para este par de chaves. Todos os dados deste certificado foram definidos na configuração do PSC. Gera-se, também, um par de chaves para ser utilizado na conexão SSL, entre o servidor e o cliente. Um certificado é gerado para esse par de chaves assinado pela chave interna do PSC.

As informações gerais do grupo de administradores são inseridas logo após o armazenamento do certificado e da chave privada cifrada na memória não volátil do PSC. Estas configurações somente serão ativadas, no final da execução do comando, se nenhum erro ocorrer.

O armazenamento da chave privada do PSC é feito cifrado com uma chave simétrica gerada randomicamente. O tamanho desta chave será o máximo permitido pelo algoritmo simétrico escolhido. Essa chave simétrica é passada pelo algoritmo de compartilhamento de segredo e dividida em m partes, conforme passado por parâmetro. Posteriormente, essas partes serão cifradas com a chave pública de cada um dos m administradores, cada um a sua.

A criação dos administradores começa agora. Para cada administrador

será gerado um par de chaves e um certificado assinado pela chave do PSC correspondente a chave, o nome do administrador é solicitado para colocar no certificado. A senha que identifica o usuário é solicitada neste momento. Lembrando que esta senha não é a mesma utilizada para acessar o smartcard, por uma questão de segurança.

Os administradores terão cada um seu smartcard, aonde será inserida a sua chave privada, o seu certificado e o certificado do PSC. Os identificadores, PINs e PUKs, utilizados em cada smartcard são gerados randomicamente. A parte do segredo correspondente a cada administrador é cifrada com sua chave pública. A idéia é guardar estas partes cifradas para serem decifradas e remontadas, posteriormente, para recuperar a chave simétrica que cifra a chave privada do PSC.

As informações de cada administrador são armazenadas em tabela própria do banco de dados, como já apresentado. Após todos serem criados e nenhum erro tiver ocorrido, é ativado o grupo de administradores do PSC.

Se qualquer erro ocorrer, a execução do comando é abortada, retornando uma mensagem contendo o motivo do erro. O processo precisa ser reiniciado, sem possibilidade de continuação.

A partir deste momento, o PSC está apto a criar o conjunto de Auditores.

4.6 Criação de Grupos de Operadores

A criação do grupo de operadores é uma tarefa que prevê a criação de um conjunto de pessoas, ao qual poderão ser atribuídas chaves para ser operacionalizadas.

Esta tarefa inicia com o envio do comando de criação de um conjunto de operadores ao PSC. O comando consiste de três argumentos: o número mínimo de operadores para recomposição do segredo, a quantidade de operadores deste conjunto e o nome identificador do grupo. O nome do conjunto de operadores é único em um mesmo PSC, ele será usado para representar este na criação das chaves.

Como qualquer tarefa administrativa, a autenticação dos administradores é obrigatória. É preciso de n administradores insiram seus smartcards, um a um, informando o número para liberação do acesso. As partes do segredo serão decifradas, remontando Ks_{ADM}. O acesso da chave privada do PSC, Kr_{PROV}, está liberado.

Autenticação realizada, os dados prévios do conjunto de operadores são

inseridos na base de dados de operadores. Lembrando que para liberar este conjunto é preciso alterar o campo id_used para 1.

A chave dos operadores é randomicamente gerada, Ks_{OPER}, e passa pelo algoritmo de compartilhamento de segredo, sendo dividido pelo número total de operadores do conjunto.

Começa a iteração com os operadores do conjunto. Para todos os operadores que serão gerados, são executados os seguintes passos:

- é solicitado a inserção do smartcard;
- são gerados randomicamente os valores para o smartcard: identificador do usuário, identificador da chave privada, o PIN e PUK;
- é solicitado a especificação de uma senha. Cuidado, esta senha não é a mesma utilizada para liberar acesso ao smartcard, como explicado na seção 4.1;
- cria-se o usuário no smartcard, com o identificador gerado anteriormente;
- gera-se um par de chaves do tamanho especificado nas configurações do PSC;
- cifra uma parte do segredo compartilhado;
- solicita ao operador a digitação de seu nome, para ser inserido no certificado;
- gera-se uma requisição de certificado com o nome do operador e os dados informados na configuração do PSC;
- gera-se um certificado da requisição anterior, assinado com a chave privada do PSC, Kr_{PROV};
- grava-se o certificado do operador e o certificado do PSC no smartcard;
- insere os dados do operador no banco de dados dos operadores;

Realizados estes passos para todos os operadores do conjunto, geram-se duas chaves aleatórias: $Ks_(OPER*)$ e $Ks_{ADM-OPER}$. Estas chaves, junto com Ks_{OPER}, passarão pela execução da operação lógica XOR.

Ks_{OPER*} é armazenado na base de dados não exportáveis. $Ks_{ADM-OPER}$ é cifrado com a chave privada do PSC e armazenado na base de dados de administradores, juntamente com o resultado da operação do XOR.

Se nenhum problema ocorrer durante a execução de todos os passos anteriores, o conjunto de operadores é ativado e está apto a ser atribuído a chaves. Qualquer erro encontrado, a execução é abortada e uma mensagem de erro retorna à aplicação cliente.

Finalizando, todas as variáveis e chaves são eliminadas da memória. Qualquer passo pode ser executado no PSC.

A criação do conjunto de auditores segue o mesmo processo, com a diferença que Ks_{OPER*} será descartado, isto é, não será armazenado na base de dados não exportáveis.

4.7 Troca de Administradores

A troca do conjunto de administradores do Provedor de Serviços Criptográficos é uma tarefa que deve ser realizada sempre que houver comprometimento de $\geq n$ ou $\geq (m - n)$ administradores.

Esta tarefa inicia com o envio do comando de troca do conjunto de administradores ao PSC. O processo precisa de duas informações como parâmetro: número mínimo de administradores para remontar o segredo e quantidade do conjunto total, respectivamente, n e m. Estes serão chamados de $n*$ e $m*$ para não serem confudidas com os valores do conjunto atual de administradores.

O processo é administrativo e precisa da autenticação de n administradores para continuar. Se efetuado com sucesso, Kr_{PROV} poderá ser aberto ao final da autenticação.

As informações gerais do novo conjunto são inseridas na base de dados de administradores.Uma chave é gerada randomicamente, constituindo Ks_{ADM}. Esta chave passa pelo compartilhamento de segredo e é dividida em $m*$ partes.

Começa a iteração com os $m*$ novos administradores deste conjunto. Para todos, os seguintes passos são executados:

- é solicitado a inserção do smartcard;
- são gerados randomicamente os valores para o smartcard: identificador do usuário, identificador da chave privada, o PIN e PUK;

- é solicitado para especificar uma senha. Cuidado, esta senha não é a mesma utilizada para liberar acesso ao smartcard, como explicado na seção 4.1;
- cria-se o usuário no smartcard, com o identificador gerado anteriormente;
- gera-se um par de chaves do tamanho especificado nas configurações do PSC;
- cifra uma parte do segredo compartilhado;
- solicita ao administrador a digitarção de seu nome, para ser inserido no certificado;
- gera-se uma requisição de certificado com o nome do administrador e os dados informados na configuração do PSC;
- gera-se um certificado da requisição anterior, assinando-o com a chave privada do PSC, Kr_{PROV};
- grava-se o certificado do administrador e o certificado do PSC no smartcard;
- insere os dados do administrador no banco de dados dos administradores;

Com todos os passos realizados com sucesso, a configuração do novo conjunto é ativada, desativando automaticamente a antiga. As variáveis e chaves utilizadas no processo são apagadas da memória retornando uma mensagem de sucesso.

A ocorrência do primeiro erro aborta a execução do processo, e retorna uma mensagem de erro.

4.8 Troca de Grupo de Operadores

A troca de grupo de operadores é a mudança dos detentores de poder de uma chave do PSC. A responsabilidade passa para outro conjunto de operadores.

Esta tarefa inicia com o envio do comando de troca do grupo de operadores ao PSC. Este comando obriga a existência de três identificadores como parâmetros: da chave a ser trocada de dono, do conjunto com a responsabilidade atual da chave e o conjunto que assumirá o controle, respectivamente $chave$, ant_oper e nov_oper.

Está é uma tarefa administrativa e a autenticação de n administradores é necessária. A reconhecimento do conjunto garante a abertura da chave privada do PSC, Kr_{PROV}.

A execução começa com a busca, no banco de dados, de chaves com as informações inerentes à $chave$. A busca resulta no conhecimento do atual grupo de operadores que tem poder sobre a chave.

O valor de ant_oper é verificado na base de dados e, posteriormente, conferido com valor carregado da base de dados de chaves.

As informações do grupo também precisam ser carregadas da base de dados de administradores, a qual contém o resultado da operação do XOR e $Ks_{ADM-OPER1}$ cifrado. Ks_{OPER1*} deve ser buscado na base de dados não exportáveis.

Decifrando $Ks_{ADM-OPER1}$, pode-se aplicar a operação lógica XOR e recuperar o valor de Ks_{OPER1}. Com a chave recuperada, a chave identificada por $chave$ pode ser carregada.

Neste ponto, repete-se o processo realizado anteriormente, mas agora para recuperação de Ks_{OPER2}, a chave do conjunto de operadores identificada por $novo_oper$. Esta chave que passará a cifrar a chave no interior do PSC.

Ao final do processo, a base de dados de chaves é atualizada e um novo conjunto de operadores detém o poder sobre a chave. As variáveis e chaves utilizadas no processo são apagadas da memória e uma mensagem de sucesso é retornada.

A ocorrência do primeiro erro aborta a execução do processo e retorna uma mensagem de erro.

4.9 Criação de Pares Chaves

A criação de pares de chave é uma tarefa administrativa e necessita da autenticação de n administradores. O par de chaves criado precisa ser atribuído a um grupo de operadores. Apenas este grupo poderá utilizar esta chave.

O processo inicia com o envio da solicitação de criação de um novo par de chaves ao PSC. Para o sucesso da solicitação, precisa ser informado dois identificadores: o nome do par de chave a ser criado e o nome do grupo de operadores que terão poder sobre a chave. O tamanho da chave também pode ser informado na chamada, mas não é obrigatório, já existe um tamanho de chave setado na configuração do PSC.

Como tarefa administrativa, o processo de autenticação dos administradores é o primeiro passo a ser realizado. Se efetuado com sucesso, a chave privada do

PSC, Kr_{PROV}, será liberada.

Algumas checagens são realizadas, a fim de constatar se o grupo de operadores informado existe, e se o identificador de chaves já não foi usado.

Checagens realizadas, os dados do conjunto de operadores são carregados do banco de dados. As informações do grupo também são carregadas do banco de dados de administradores, como $Ks_{ADM-OPER}$ cifrada e o resultado da operação lógica XOR. Ks_{OPER*} é selecionada da base de dados não exportável.

$Ks_{ADM-OPER}$ é decifrada e a operação do XOR já pode ser realizada, possibilitando a recuperação de Ks_{OPER}. Com a chave do conjunto de operadores recuperada, o par de chaves é criado.

A chave privada é armazenada do sistema de arquivos cifrada com Ks_{OPER}, juntamente com a chave pública. As informações da chave são inseridas no banco de dados de chaves.

A criação de pares de chaves é simples. Os pontos interessantes do processo são:

- possibilidade de criar chave de tamanho diferente da especificada na configuração do PSC;
- aplicação da operação lógica XOR para recuperar o segredo do conjunto de operadores, Ks_{OPER};
- checagem da não existência de Ks_{OPER*} para aplicação do XOR(vide seção 4.11);

4.10 Utilização dos Pares de Chaves

A utilização dos pares de chaves gerenciadas é uma tarefa realizada pelo conjunto de operadores responsável. Lembrando, toda chave é atribuída a um conjunto de operadores no momento de sua criação(vide seção 4.9).

O processo inicia com o envio da solicitação de uso de uma chave ao PSC. Os parâmetros para execução da operação são:

- o nome da chave a ser utilizada;

- nome do arquivo que será assinado, podendo conter informações ou um hash já calculado (caminho do arquivo no computador que está executando o cliente da AG. O arquivo será enviado para o servidor);

O primeiro passo é buscar os dados da chave informada, para conhecer o conjunto de operadores que detém o seu poder. A autenticação dos operadores é então solicitada, resultando na remontagem de Ks_{OPER}.

A chave privada gerenciada já pode ser carregada, decifrando com Ks_{OPER}.

Uma iteração com a aplicação cliente acontece para buscar o arquivo para assinar. O conteúdo do arquivo pode ser de duas formas: um hash já calculado, que é passado diretamente ao servidor, ou um arquivo texto. No caso do arquivo texto, o hash é calculado no cliente, e então passado o resultado para o servidor.

Recebido o hash do cliente, o servidor pode realizar o processo de assinatura, devolvendo o resultado, finalizando a execução da tarefa. O resultado será gravado em um arquivo com o mesmo nome do arquivo original, com a extensão $.sign$.

4.11 Cópia de Segurança

As cópias de segurança servem para manter em lugar e forma segura os dados do PSC, se por acaso ocorrer um desastre, a continuidade das atividades do provedor não será inviabilizada.

O processo inicia com a solicitação de cópia de segurança ao PSC. O parâmetro obrigatório para execução é o novo valor para remontagem do segredo do conjunto de administradores, para recuperação da cópia de segurança. O valor será l e deverá seguir os seguintes critérios: $1 \leq n \leq l \leq m$, sendo que $m - l < n$.

Realizadas as checagens de parâmetros, tratando-se de uma tarefa administrativa, a autenticação dos administradores é obrigatória. Liberando ao final do processo de reconhecimento o acesso a Kr_{PROV}.

As partes dos segredos cifrados, as chaves armazenadas (incluindo certificados) e os bancos de dados (excluindo o banco que contém os dados não exportáveis) são copiados formando um pacote com todas as informações do provedor. Sobre o pacote aplica-se uma função de resumo, resultando um valor de hash.

A chave de sessão, Ks_{BKP}, é gerada aleatoriamente. O pacote dos dados será cifrado com esta chave e armazenado no pacote final do backup. O hash do pacote será assinado por $KrPROV$, para posterior checagem de integridade e é adicionado também ao pacote final.

A chave privada do provedor é cifrada por Ks_{BKP} e adicionada ao pacote final, juntamente com o certificado auto-assinado do provedor.

A chave de sessão da cópia, Ks_{BKP}, é dividida em m partes pelo algoritmo de compartilhamento de segredo. Os dados gerais do backup são inseridos na base de dados do backup.

Começa a iteração com a chave pública dos $m*$ administradores. Para cada um, os seguintes passos são executados:

- os dados do administrador são selecionados da base de dados de administradores;
- o certificado do administrador é carregado e a chave pública é extraída;
- a parte do segredo é cifrado com a chave pública do administrador;
- a parte cifrada e o certificado do administrador são inseridos no pacote final do backup;
- os dados dos administradores do backup são inseridos na base de dados de backup;

Realizados todos os passos com os administradores, o backup é ativado na base de dados, isto é, o campo id_used é alterado para 1. Esta base é adicionada ao pacote final de dados.

O pacote final está agora pronto para ser extraído do PSC com segurança, sendo solicitada a inserção do token de backup na porta USB. O pacote é inserido no token e a cópia de segurança do provedor é realizada, retornando uma mensagem de sucesso.

Se ocorrer qualquer problema durante o processo, a execução é abortada retornando uma mensagem de erro.

4.12 Recuperação da Cópia de Segurança

A recuperação da cópia de segurança será realizada sempre que o Provedor de Serviços Criptográficos estiver comprometido, reconstruindo todo o ambiente

do gerenciamento de chaves, dando continuidade às atividades do provedor.

Esta tarefa inicia com a solicitação de recuperação de cópia ao PSC. Os parâmetros para esta função são:

- n - o valor de número mínimo para recomposição do segredo para o novo conjunto de administradores;
- m - o número de administrador do novo conjunto.

O primeiro requisito, após iniciado o processo, é a inserção do token de backup. Nele contém o pacote final da cópia de segurança, realizado na seção 4.11. Este pacote será carregado do token, dando início à recuperação.

Com o pacote já no PSC, é exigido a autenticação de l administradores, valor definido na seção 4.11. A autenticação permite a reconstrução de Ks_{BKP}, que será usado para decifrar as bases de dados do provedor. Aplica-se uma função de resumo sobre as bases, gerando o $hash1$.

A autenticação possui algumas particularidades em relação as outras. Estas diferentes são inerentes à garantia da não existência e duas instâncias do PSC, sendo operacionalizadas paralelamente. Os pontos são:

- a senha de acesso ao smartcard (PIN) é alterado para todos os administradores autenticadas;
- a nova senha é gerada randomicamente. A antiga e a nova senha são armazenados na base de backup, em uma tabela temporária, juntamente com os identificadores dos smartcards de cada um.
- o armazenamento é necessário para o caso de ocorrer algum problema na recuperação da cópia de segurança, depois de autenticado os administradores. Com os PINs para acesso a chave privada dos smartcards alterados, o PSC antigo não poderia ser mais operacionalizado, e a cópia também não poderia ser recuperada. Esse processo deve ser realizado com muita atenção, para não acontecer maiores problemas.

O certificado auto-assinado, também contido no pacote, é carregado, e retirado Ku_{PROV}. A chave pública do provedor permite a verificação da assinatura do hash das bases existentes também no pacote. Se validada, este hash é comparado a $hash1$, garantindo a integridade das bases de dados.

Ainda com Ks_{BKP}, a chave privada do PSC pode ser recuperada e o novo conjunto de administradores começa a ser criado. Gera-se Ks_{ADM} randomicamente e o divide em m partes pelo algoritmo de compartilhamento de segredo. Os dados gerais do novo conjunto são inseridos na base de dados de administradores.

Agora para cada administrador, os seguintes passos são realizados:

- é solicitada a inserção do smartcard do administrador;
- são gerados randomicamente os valores para o smartcard: identificador do usuário, identificador da chave privada, o PIN e o PUK;
- é solicitado para o administrador especificar uma senha. Cuidado, esta senha não é a mesma utilizada para liberar acesso ao smartcard, como explicado na seção 4.1;
- cria-se o usuário no smartcard, com o identificador gerado no passo 4.12;
- gera-se um par de chaves do tamanho especificado nas configurações do PSC no smartcard;
- cifra com a chave pública do administrador uma parte do segredo compartilhado;
- solicita ao administrador digitar seu nome, para ser inserido no certificado;
- gera-se uma requisição de certificado com o nome do administrador e os dados informados na configuração do PSC;
- gera-se um certificado da requisição anterior, assinado-o com a chave privada do PSC, Kr_{PROV};
- grava-se o certificado do administrador e o certificado do PSC no smartcard;
- insere os dados do administrador no banco de dados dos administradores;

Finalizados m vezes, os passos acima, o conjunto é ativado, possibilitando o seu uso. A restauração da cópia de segurança, neste momento, foi realizada com sucesso retornando uma mensagem.

A ocorrência de um problema, aborta a operação retornando uma mensagem de erro. Se os administradores do backup já estiverem autenticados, um mecanismo de recuperação dos PINs de seus smartcards é executado.

O mecanismo solicita a inserção de todos os smartcards utilizados na autenticação e restaura os PINs antigos. Estes PINs são carregados da base de dados temporários do backup.

4.13 Funções Auxiliares

A Aplicação Gestora possui algumas funções auxiliares, isto é, funções que não foram especificadas nos mecanismos de gerenciamento de chave, mas que auxiliam na operacionalização do Provedor de Serviços Criptográficos.

4.13.1 Listagem dos Grupos de Operadores

Esta função, quando solicitada ao PSC, imprime uma listagem dos conjuntos de operadores existentes. Esta listagem contém o nome identificador do conjunto, o número mínimo para reconstrução do segredo e a quantidade de componentes. Não é necessária a autenticação de nenhum grupo.

4.13.2 Listagem dos Operadores de um Grupo

A execução desta função necessita de um parâmetro: o identificador de um conjunto de operadores. Ela irá apresentar uma listagem com os membros do conjunto especificado.

A listagem irá conter o nome de cada operador informado no momento da sua criação. Antes de selecionar os dados do banco de operadores, o identificador do conjunto é validado. Não é necessária a autenticação de nenhum grupo.

4.13.3 Listagem das Chaves Gerenciadas

A invocação deste processo percorre todas as chaves gerenciadas pelo PSC. O nome identificador das chaves é impresso, juntamente com o nome do grupo de operadores com poder sobre elas.

Adicionalmente, a chave pública de cada par é informada. Não é necessária a autenticação de nenhum grupo.

4.13.4 Ativação dos Conjuntos de Operadores

A ativação dos conjuntos de operadores deve ser realizada para todos os conjuntos de operadores, após recuperação da cópia de segurança (vide seção 4.12). Este processo faz parte da rastreabilidade das chaves existente no PSC.

Esta tarefa inicia com a solicitação de ativação ao PSC. O identificador do conjunto deve ser passado como parâmetro.

A recomposição dos dados não exportáveis, isto é, a ativação do conjunto de operadores, deve ser feita com a autenticação do conjunto de administradores e o conjunto de operadores informado na chamado do processo.

Autenticado o conjunto de administradores, Kr_{PROV} estará liberado para uso. Após checado a existência do conjunto de operadores, e reconhecidos, Ks_{OPER} pode ser reconstruída.

$Ks_{ADM-OPER}$ cifrado e o resultado da aplicação lógica do XOR são carregados da base de dados de administradores. A chave de ligação dos administradores com o conjunto de operadores, $Ks_{ADM-OPER}$, podem ser decifrados por Kr_{PROV}.

Utilizando a característica de reversibilidade do XOR, aplica-se sobre o resultado carregado da base de dados de administradores, $Ks_{ADM-OPER}\ oplus\ Ks_{OPER}\ oplus\ Ks_{OPER*}$, as chaves $Ks_{ADM-OPER}$ e Ks_{OPER}, recuperando o valor de Ks_{OPER*}.

A chave recuperada pode agora ser armazenada no banco de dados não exportáveis e o processo de ativação finalizado. Uma mensagem de sucesso da execução retorna. Qualquer problema que venha a ocorrer, aborta a tarefa de ativação e retorna uma mensagem de erro.

4.13.5 Listagem do Conteúdo de um Smartcard

Os smartcards, como mostrado na seção 4.1, são organizados internamente através de um sistema de arquivos. As chaves e os certificados viram cada um, um arquivo.

Este processo mostra todo o conteúdo de um smartcard, incluindo usuário, chaves e certificados. Não é necessária a autenticação de nenhum grupo.

4.13.6 Serviços Criptográficos

O Provedor de Serviços Criptográficos, além de operacionalizar o ciclo de gerenciamento de chaves, também poderá prover a execução de algoritmos criptográficos básicos, tais como: criptografia simétrica, funções resumo e geração de número randômicos.

A utilização destas funções no PSC garante a qualidade dos algoritmos. Em outros equipamentos, estes processo podem estar comprometidos.

Capítulo 5

Conclusões

O desenvolvimento de uma Aplicação Gestora para o gerenciamento de chaves criptográficas não é uma tarefa trivial, necessitando de amplo conhecimento. Contudo, os objetivos propostos para o trabalho foram alcançados.

Um protótipo funcional foi desenvolvido propiciou a validação dos mecanismos utilizados. A linguagem C, inicialmente desconhecida, foi amplamente estudada e adquirido conhecimento para sua correta utilização.

A fase de implementação deve ser complementada com outra mais intensiva de testes. O problema resolvido requer um nível de segurança alto, por trabalhar com chaves para ambientes com alto valor agregado.

O conhecimento agregado sobre smartcard, possibilitou o desenvolvimento de uma biblioteca, que está sendo comercializada e utilizada por empresas, fazendo parte dos seus produtos.

Concluindo, o estudo de Provedor de Serviços Criptográficos pode evoluir, com os seguintes trabalhos futuros:

- desenvolvimento de uma interface para utilização das chaves gerenciadas pelo PSC para o OpenSSL. O OpenSSL é a biblioteca mais utilizada para funções criptográficas, e isso tornaria o provedor compatível com os principais equipamentos e programas do mercado;

- integração da Infra-estrutura de Chaves Públicas desenvolvida no projeto ICP-EDU I, possibilitando a criação de Autoridades Certificadores utilizando PSCs;

- desenvolvimento de uma interface gráfica para gerenciamento do PSC. Isso tornaria

mais iterativa e prática a utilização;

- incrementar o módulo de utilização de smartcards, possibilitando o uso de diversos leitores e diversas versões de cartões;

Referências Bibliográficas

[1] DIAS, J. da S. *Confiança no Documento Eletrônico*. Tese (Doutorado) — Universidade Federal de Santa Catarina, Setembro 2004.

[2] WIKIPÉDIA. *Criptografia*. maio 2005. Disponível em: <http://pt.wikipedia.org/wiki/Criptografia>.

[3] HOUSLEY, R.; POLK, T. *Planning for PKI: Best Pratices Guides for Deploying Public Key Infrastructure.* [S.l.]: Wiley, 2001.

[4] WIKIPÉDIA. *Criptografia de Chave Pública*. Maio 2005. Disponível em: <http://pt.wikipedia.org/wiki/Criptografia_assimétrica>.

[5] RIVEST, R.; SHAMIR, A.; ADELMAN, L. *A Method for Obtainig Digital Signatures and Public-Key Cryptosystems*. 1977.

[6] GROUP, N. W. *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. [S.l.], Janeiro 1999.

[7] TECHNET, M. *Infra-estrutura de Chave Pública*. Janeiro 2005. Disponível em: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/pt-br/library/ServerHelp/32aacfe8-83af-4676-a45c-75483545a978.mspx>.

[8] GROUP, N. W. *Enhanced Security Services for S/MIME*. [S.l.], Junho 1999. Disponível em: <http://www.ietf.org/rfc/rfc2634.txt>.

[9] GROUP, N. W. *IP Security Document Roadmap*. [S.l.], Novembro 1998. Disponível em: <http://www.ietf.org/rfc/rfc2411.txt>.

[10] GROUP, T. W. *Transport Layer Security*. [S.l.], Maio 2005. Disponível em: <http://www.ietf.org/html.charters/tls-charter.html>.

[11] TECHNET, M. *Visão geral sobre certificados*. Janeiro 2005. Disponível em: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/pt-br/library/ServerHelp/a7b4cbea-7c3a-4bf5-b427-bff2ea8bb0f3.mspx>.

[12] RNP et al. *ICP-EDU II Módulo de Hardware e Serviços Seguros em Redes de Computadores*. Agosto 2004. Disponível em: <http://www.rnp.br/_arquivo/documentos/pal0219.pdf>.

[13] ANOREG. *Site Oficial da ANOREG*. Junho 2005. Disponível em: <http://www.anoregbr.org.br/>.

[14] TECNOLOGIAS, K. *Site Oficial da Kryptus Tecnologias*. Junho 2005.

[15] ITI. *Site Oficial do Instituto Nacional de Tecnologia da Informação*. Junho 2005. Disponível em: <http://www.iti.br/>.

[16] *Medida Provisória 2.200-2*. Medida Provisória que instituíu a ICP-BRASIL.

[17] MARTINI, R. *Anteprojeto - Construção de Plataforma Criptográfica Aberta para a ICP-Brasil.* Outubro 2003. Renato.Martini@planalto.gov.br.

[18] RNP, R. N. d. P. *GT ICP-EDU*. 2003. Disponível em: <http://www.rnp.br/pd/gts2003-2004/gt-icp.html>.

[19] RNP, R. N. d. P. *GT ICP-EDU II*. Maio 2005. Disponível em: <http://www.rnp.br/pd/gts2004-2005/chaves_publicas.html>.

[20] MARTINA, J. E. *Projeto de um Provedor de Serviços Criptográficos Embarcado para Infra-estrutura de Chaves Públicas e suas Aplicações*. Dissertação (Mestrado) — UFSC, 2005.

[21] HORNIG, C. *A Standard for the Transmission of IP Datagrams over Ethernet Networks*. [S.l.], Abril 1984.

[22] CALIFORNIA, I. S. I. U. of S. *Dod Standard Transmission Control Protocol*. [S.l.], Janeiro 1980. Disponível em: <http://www.ietf.org/rfc/rfc0761.txt>.

[23] GROUP, T. L. S. W. *The SSL Protocol Version 3.0*. [S.l.], Novembro 1996. Disponível em: <http://wp.netscape.com/eng/ssl3/draft302.txt>.

[24] IEC/ISO, M. of. *ISO/IEC 7816-4 Interindustry command for interchange*. [S.l.], Novembro 1998. Disponível em: <http://www.ttfn.net/techno/smartcards/iso7816_4.html>.

[25] LABORATORIES, R. *PKCS #15 v1.1 Standard*. [S.l.], Junho 2000. Disponível em: <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-15/index.html>.

[26] ASSOCIATION, I.-S. *IEEE POSIX 1003.1c standard - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) - Amendment 2: Threads Extension [C Language]*. 1995.

[27] PROJECT, T. O. *Site Oficial do OpenCT*. Maio 2005. Disponível em: <www.opensc.org>.

[28] PROJECT, T. O. *Site Oficial do OpenSC*. Maio 2005. Disponível em: <www.opensc.org>.

[29] RESEARCH, A. S. *Site Oficial do SQLite*. Maio 2005. Disponível em: <www.sqlite.org>.

[30] CORPORATION, D. E. *Database Language SQL*. Julho 1992. Disponível em: <http://www.contrib.andrew.cmu.edu/ shadow/sql/sql1992.txt>.

[31] KARRMANN, S. *Site Oficial da Sharesecret*. Maio 2005. Disponível em: <http://www.mathematik.uni-ulm.de/m5/sk/sharesecret.html>.

[32] PROJECT, T. O. *Site Oficial do OpenSSL*. Maio 2005. Disponível em: <www.openssl.org>.

[33] PROJECT, O. *Site Oficial do OpenSSH*. Maio 2005. Disponível em: <http://www.openssh.com/>.

[34] ALLIANCE, T. O. *Site Oficial do OpenPGP*. Maio 2005. Disponível em: <http://www.openpgp.org/>.

[35] FOUNDATION, E. *Site Oficial do Eclipse*. Maio 2005.

[36] HEESCH, D. van. *Site Oficial do Doxygen*. Maio 2005. Disponível em: <http://www.stack.nl/ dimitri/doxygen/>.

Apêndice A

Anexos