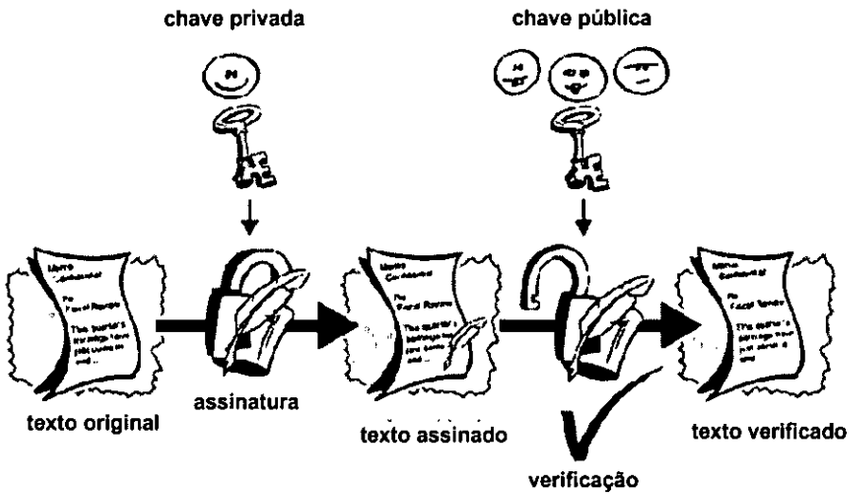
UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA
CURSO DE INFORMÁTICA

Trabalho de Licenciatura

Introdução da Certificação Digital na Rede Electrónica do Governo



Discente: **Eugénio António Jeremias**

Maputo, 2005

UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA
CURSO DE INFORMÁTICA

Trabalho de Licenciatura

Introdução da Certificação Digital na Rede Electrónica do Governo

Discente: **Eugénio António Jeremias**

Supervisor: **dra. Judite Mandlate**

Co-supervisor: **Eng. Lourino Chemane**

Maputo, 2005

DEDICATÓRIA

Dedico este trabalho à minha família que ajudou-me a superar os obstáculos ao longo da minha carreira: minha mãe Joaquina Francisco, meus irmãos Horácia, Rui, Joana, Virgínio, minha sobrinha Dinha, minha esposa Nicole e em especial ao meu pai, António Jeremias que sempre apostou em mim e acreditou que um dia eu alcançaria este feito.

AGRADECIMENTOS

Quero agradecer primeiro aos meus supervisores pelo empenho que tiveram durante a elaboração do presente trabalho.

Ao eng. Eneas Hunguana, pelo apoio incondicional prestado na definição do tema do trabalho, elaboração do protocolo e apoio durante a elaboração do trabalho.

A Dra. Esselina Macome, pela orientação e motivação para a elaboração do trabalho.

Ao eng. Sérgio Carrilho da UTICT pela assistência na elaboração do modelo PKI.para a GovNet.

Ao dr. Nelson Mazibe, pelas suas sugestões e críticas ao trabalho.

E a todos os que apoiaram e motivaram-me directa ou indirectamente a destacar o Dr. António Sopa.

DECLARAÇÃO DE HONRA

Declaro por minha honra que este trabalho é fruto da minha profunda investigação e não foi submetido para outro grau que não seja o indicado, Licenciatura em Informática no Departamento de Matemática e Informática da Universidade Eduardo Mondlane.

Maputo, Outubro 2005

O autor

Eugénio António Jeremias

RESUMO

A segurança em uma rede de computadores está relacionada com a necessidade da protecção da informação e do equipamento contra a leitura, escrita ou qualquer tipo de manipulação não autorizada. Com a utilização da Internet em ambiente corporativo e a abertura para o mundo externo, a preocupação e o risco de invasão aos sistemas corporativos aumentam.

Para garantir a segurança de uma rede de computadores é necessário aplicar vários mecanismos de segurança, como por exemplo: autenticação, controle de acesso, sistemas de detecção de intrusão, antivírus, *firewall,* criptografia da informação e utilizar os certificados digitais.

A criptografia por chave pública resolve efectivamente o problema da confidencialidade da informação transmitida mas não atende aos requisitos de integridade, autenticidade e deixa incertezas sobre a obtenção, reconhecimento, validade e distribuição das chaves utilizadas (GOLDANI, 2000).

Como forma de sanar estas inconveniências foi criada uma estrutura de segurança, designada por Infra-estruturas de Chave Pública (*Public Key Infrastructure (PKI)*), baseada na utilização dos certificados digitais. O certificado digital é um documento que contém os dados de identidade pessoal e a chave pública do seu titular, garantindo desta forma a sua correspondência.

O presente trabalho propõe um modelo de PKI para a Rede Electrónica do Governo (GovNet) de modo a possibilitar a emissão, gestão e utilização de certificados digitais com a finalidade de garantir a confidencialidade, autenticidade, integridade e não repúdio da informação emitida.

O modelo proposto de PKI para GovNet é constituído por três entidades: Autoridade Gestora - cujo a função é definir, avaliar e aprovar políticas e normas no âmbito da PKI; Autoridade Certificadora – cujo a função é emitir, distribuir, revogar, renovar e gerir os certificados digitais e a Autoridade de Registo – que age como interface da PKI com o usuário e compete-lhe identificar, registar os usuários da PKI e encaminhar à Autoridade Certificadora os registos para a emissão de certificados.

Para garantir a interoperabilidade da PKI em diferentes plataformas e aceitabilidade internacional, para além da não vinculação a soluções proprietárias, a implementação da PKI da GovNet deve basear-se em padrões e protocolos usados internacionalmente e que tornam a comunicação consistente.

A introdução da certificação digital na GovNet será um importante mecanismo de segurança para o fornecimento de serviços de autenticação e geração de provas para além de garantir a confidencialidade, integridade e validade jurídica dos documentos electrónicos.

SIGLAS E ABREVIATURAS

AC	Autoridade Certificadora
AC-Raiz	Autoridade Certificadora Raiz
AG	Autoridade Gestora
API	*Application Programming Interface*
AR	Autoridade de Registo
DAP	*Directory Access Protocol*
DES	*Data Encryption Standard*
DSA	*Digital Signature Algorithm*
DMZ	*Demilitarized Zone*
DN	*Distinguished Name*
DNS	*Domain Name System*
GovNet	Rede Electrónica do Governo
HSM	*Hardware Security Module*
HTTP	*Hypertext Transport Protocol*
HTTPS	*Hypertext Transport Protocol Secure*
IBM	*International Business Machines*
IDS	*Intrusion Detection System*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IMAP	*Internet Message Access Protocol*
IP	*Internet Protocol*
IPSec	*IP Security*
ISA	*Internet Security and Acceleration*
ISAKMP	*Internet Security Association and Key Management Protocol*
ISO	*International Organization for Standardization*
ITU	*International Telecommunication Union*
LAN	*Local Area Network*
LCRs	Lista de Certificados Revogados
NDS	*Novel Directory Services*
LDAP	*Lightweight Directory Access Protocol*
OCSP	*On-line Certificate Status Protocol*
PGP	*Pretty Good Privacy*
PHP	*Hypertext Preprocessor*

PIN	*Personal Identification Number*
PKCS	*Public Key Cryptography Standard*
PKI	*Public Key Infrastructure*
PKIX	*Internet X.509 Public Key Infrastructure*
POP3	*Post Office Protocol, version 3*
RFC	*Request For Comments*
RSA	Rivest, Shamir, and Adleman
SET	*Secure Electronic Transactions*
SGDB	Sistema Gerenciador de Base de Dados
SMTP	*Simple Mail Transfer Protocol*
SPKI	*Simple Public Key Infrastructure*
SQL	*Structure Query Language*
SSH	*Secure Shell*
SSL	*Secure Socket Layer*
S/MIME	*Secure Multipurpose Internet Mail Extensions*
TCP/IP	*Transmission Control Protocol / Internet Protocol*
TLS	*Transport Layer Security*
UDP	*User Datagram Protocol*
USB	*Universal Serial Bus*
UTICT	Unidade Técnica de Implementação da Política de Informática
VLAN	*Virtual Local Area Network*
VPN	*Virtual Private Network*
WWW	*World Wide Web*

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

1. INTRODUÇÃO

A adesão à rede mundial de computadores provocou uma mudança profunda no comportamento de pessoas, instituições e governos. Surgiram novos hábitos e métodos na forma como as tarefas do dia-a-dia são realizadas. São exemplos práticos, os novos métodos de troca de correspondência assim como certas transacções comerciais, actividades que nos dias que correm já podem ser realizadas electronicamente, através das redes de computadores.

Estes novos recursos trouxeram consigo novos desafios, no que diz respeito à área da segurança: é preciso garantir a confidencialidade, integridade, autenticidade e disponibilidade da informação nas transacções realizadas através das redes de computadores no geral, e pela Internet em particular. O Governo deve elaborar políticas tecnológicas que visam desenvolver infra-estruturas para que mais pessoas sejam incluídas na sociedade virtual (ITI, 2005). Neste âmbito, o Governo de Moçambique com vista a modernizar e tornar eficientes as transações do Governo e os serviços ao cidadão, criou a Rede Electrónica do Governo (GovNet) que se encontra na fase inicial de implementação.

A GovNet é uma infra-estrutura de comunicação electrónica que servirá de suporte para a implementação de sistemas de informação e implantação de todas as aplicações tecnológicas de apoio às actividades de coordenação do Governo com outros sectores de utilidade pública (UTICT, 2005).

Uma das acções para conferir maior segurança nas transacções realizadas na GovNet é o estabelecimento de uma Infra-estrutura de Chave Pública (*Public Key Infrastructure* (PKI)) que é uma arquitectura, baseada na utilização de Certificados Digitais, capaz de assegurar a identidade de cada indivíduo na rede e garantir a confidencialidade, integridade e não-repudiação das transações e documentos electrónicos, para além de permitir o reconhecimento jurídico dos mesmos.

O Certificado Digital é um arquivo que contêm os dados sobre um indivíduo ou instituição que o utiliza para comprovar a sua identidade perante terceiros, e vice-versa (PINHO, ?). Funciona como um bilhete de identidade electrónico, permitindo que uma transacção electrónica realizada via Internet torne-se segura, uma vez que as partes envolvidas deverão apresentar mutuamente as suas credenciais, comprovando as suas identidades.

A adopção da certificação digital representa um importante passo na ampliação da prestação de serviços públicos e modernização do Estado. Permite eliminar de forma substancial a necessidade da tramitação de papéis, o que significa economia de tempo, espaço físico para o armazenamento dos documentos, redução de custos de impressão e da burocracia, através da automatização de determinados processos (PINHO, ?).

O presente trabalho aborda no capítulo 2 as questões relativas a necessidade e mecanismos de protecção da informação em redes de computadores. O capítulo 3, apresenta os conceitos, padrões e detalhes sobre a composição e funcionamento de uma PKI. O capítulo 4, constitui o cerne do presente trabalho, apresenta o modelo proposto da PKI para a GovNet, seguindo padrões rígidos e normas internacionais, com vista a criar um ambiente para emissão e gestão de certificados digitais interoperável e aceitável internacionalmente. Em anexo, para além do glossário, é apresentada a avaliação e selecção do *software* de PKI, a instalação de um Certificado Digital no *browser*, os requisitos de *software e hardware* com vista a implementação do modelo proposto e o interface *web* da solução PKI sugerida.

1.1 Descrição do Problema

Actualmente em Moçambique, não há reconhecimento jurídico dos documentos electrónicos, assim como das transações electrónicas devido a ausência da legislação inerente. Este facto, aliado à insegurança e desconfiança no meio digital, devido a ausência de alguns mecanismos apropriados que elevam o grau de segurança, não permite a realização de transacções electrónicas seguras e o desenvolvimento do comércio electrónico.

Os documentos, na sua diversidade, são produzidos através de meios digitais (computador) e é imperioso que sejam impressos em papel para serem assinados de modo a adquirirem a sua validade legal.

No caso da correspondência pelo correio electrónico, no nosso país não existem mecanismos para verificar a identidade do remetente de uma mensagem, podendo a mensagem original ser interceptada por intrusos, ser alterada e enviada ao destinatário, que a receberá e não terá como verificar a sua integridade e a verdadeira origem.

A GovNet visa estabelecer uma infra-estrutura de comunicação electrónica (UTICT, 2005), no entanto irá se basear na transação e partilha de documentos no formato electrónico que carece do reconhecimento jurídico e de procedimentos apropriados para garantir a autenticidade e integridade dos mesmos. Deste modo não haverá confiança nas transações realizadas e não será possível, por exemplo, realizar transações comerciais por via electrónica.

1.2 Objectivos

1.2.1 Objectivo Geral

Estudar e propor um modelo de Infra-estrutura de Chave Pública para a Rede Electrónica do Governo (GovNet) de forma a possibilitar a emissão e utilização de certificados digitais para conferir maior segurança nas transacções electrónicas.

1.2.2 Objectivos Específicos

- Estudar a segurança em redes de computadores e a Infra-estrutura de Chave Pública;
- Definir os requisitos de certificados na GovNet;
- Propor a arquitectura de Infra-estrutura de Chave Pública para a GovNet;
- Estabelecer uma hierarquia das Autoridades de Certificação
- Definir os serviços de certificados na GovNet;
- Elaborar a política de certificados na GovNet;
- Avaliar as soluções de software existentes para a implementação da PKI da GovNet.
- Especificar os requisitos de hardware para a implementação das Autoridades de Certificação

1.3 Metodologia

Para a materialização dos objectivos anunciados foram realizadas as seguintes etapas:

- Pesquisa e consulta bibliográfica;
- Estudo teórico;
- Concepção do modelo da PKI para a GovNet com base nos conhecimentos adquiridos no estudo teórico;
- Pesquisa e avaliação das soluções de software existentes para a implementação de uma PKI, quer comerciais assim como as gratuitas de modo a identificar a solução ideal, tendo em consideração os seguintes pontos:
  - Aderência aos padrões existentes actualmente na GovNet;
  - Funcionalidades e independência a plataforma de implementação;
  - Flexibilidade de alteração;
  - Solução não proprietária; e
  - Documentação da solução.

A pesquisa e consulta bibliográfica, assim como o estudo teórico, cujo o resultado é apresentado no capítulo 3, permitiram o entendimento profundo sobre a composição e funcionamento de uma PKI.

1.4 Resultado Esperado

O presente estudo terá como resultado o modelo proposto de PKI para a GovNet constituída por:

- Arquitectura da PKI para a GovNet;
- Política de certificados;
- Declaração de Práticas de Certificação;
- Selecção do software para a implementação da PKI e descrição das suas características;
- Requisitos de hardware para a implementação das Autoridades de Certificação.

A instituição beneficiária será Unidade Técnica de Implementação da Política de Informática (UTICT) que está a implementar a infra-estrutura da GovNet.

2. SEGURANÇA EM REDES DE COMPUTADORES

2.1 INTRODUÇÃO

Este capítulo apresenta os aspectos relevantes a ser observados para garantir a segurança em redes de computadores, dando maior ênfase a identificação das vulnerabilidades, ameaças e ataques e a abordagem sobre os mecanismos para neutralizar os ataques.

A segurança em uma rede de computadores está relacionada à necessidade da protecção do equipamento e da informação, contra a leitura, escrita ou qualquer tipo de manipulação não autorizada. Também está intimamente relacionada com o comportamento humano e tem ganho uma importância cada vez maior com a utilização crescente das redes de computadores.

O acesso remoto ao *site*[1] de uma organização permite aos utilizadores aceder serviços e a informação necessária para realizar as suas actividades estando fora do edifício ou do site da organização. Porém, a garantia de que a informação será acedida apenas pelo seu proprietário ou pessoa autorizada tornou-se numa questão preocupante no seio das corporações.

A informação nos dias actuais é um dos activos de maior importância no universo das organizações, consequentemente as medidas para a sua protecção devem ser intensivamente aperfeiçoadas, tanto no que diz respeito à segurança lógica, que é implementada através de software, assim como a segurança física, relacionada a protecção dos recursos contra roubo, sabotagem, vandalismo, incêndio, humidade, etc.

Neste contexto, segundo SYMANTEC (2004), a segurança da informação é uma prioridade corporativa porque é um elemento chave e passa a ser um requisito estratégico que interfere na capacidade das organizações realizarem negócios e no valor de seus produtos no mercado.

[1] Site é um conjunto de computadores conectados.

2.2 CONCEITOS PRINCIPAIS

Como forma de estreitar a compreensão das partes subsequentes do presente trabalho, esta secção apresenta as premissas e conceitos principais de segurança utilizados.

Activo: é tudo aquilo que tem valor e desta forma requer protecção (NETO, 2003). Como exemplo de activos temos os elementos que compõem uma rede (computadores, impressoras, hubs, roteadores, etc.). A informação é dos activos mais valiosos no universo das organizações.

Ameaça: é todo o mecanismo que pode ser usado para explorar uma vulnerabilidade.

Autenticação: garantia de que a origem de uma informação seja inequívoca e correctamente identificada;

Autorização: permissão ao acesso da informação e recursos disponíveis, dependendo dos direitos exclusivos de cada usuário;

Confidencialidade: garantia de que a informação é acessível apenas a pessoas devidamente autorizados;

Disponibilidade: garantia de que os usuários autorizados tenham acesso a informação sempre quando requerido;

Integridade: consiste em assegurar que a informação seja modificada ou apagada por pessoas autorizadas.

SEGURANÇA: consiste em garantir a autenticação, confidencialidade, Integridade e disponibilidade da informação;

Controle de Acesso: garantia de que o acesso a informação seja controlado pelo sistema que a hospeda ou transmite;

Não-repudiação: garantia de que a origem e o destino de uma informação não a repudiem durante os processos de transmissão;

Privacidade: é ter controle sobre as informações pessoais/privadas e exercer este controle de forma consistente de acordo com os interesses pessoais.

Risco: é tudo aquilo que pode afectar os negócios e impedir que os objectivos sejam alcançados.

Intrusão/Invasão: é o acesso intencional e não autorizado ao sistema ou serviço.

2.1 VULNERABILIDADES

Vulnerabilidade é um ponto fraco de um activo ou grupo de activos, onde uma ameaça aproveita este ponto fraco para causar danos ao activo (CANDÉA, 2002).

É necessário realizar uma verificação das vulnerabilidades para apurar se activos são seguros ou não, e para poder-se concretizar a avaliação de riscos (vide 2.5). Os riscos não podem ser determinados sem o conhecimento de até que ponto um sistema é vulnerável, à acção das ameaças.

As vulnerabilidades podem ser encontradas no modo de agir dos usuários, nos equipamentos e nos *softwares*. Por exemplo, não observar os cuidados para protecção da *password* má configuração ou defeitos de um *software*.

2.2 AMEAÇAS E ATAQUES

As ameaças são mecanismos que actuam nas vulnerabilidades do activo causando perdas ou danos ao mesmo. A realização de uma ameaça intencional constitui um ataque (CANDÉA, 2002).

Segundo LAURENEANO (2002), um atacante pode ter vários objectivos ao realizar um ataque como: destruição, modificação ou roubo da informação para além da interrupção de serviços ou procurar vulnerabilidades no sistema para depois explorá-las.

Para garantir a protecção de uma rede é importante conhecer as ameaças e técnicas de ataques utilizados pelos invasores, para então aplicar as medidas e ferramentas adequadas para a protecção desses recursos.

Algumas das principais ameaças e ataques que podem ocorrer numa rede de computadores são os seguintes:

Personificação: uma entidade faz-se passar por outra a fim de obter privilégios de forma fraudulenta;

Replay: uma mensagem, ou parte dela, é interceptada e posteriormente transmitida para produzir um efeito não autorizado;

Modificação: o conteúdo de uma mensagem é alterado sem que o sistema e o usuário consigam detectar a alteração;

Recusa ou **Impedimento do Serviço:** ocorre quando uma entidade actua de forma a impedir que as entidades autorizadas tenham acesso aos recursos;

Ataques Internos: ocorrem quando usuários legítimos comportam-se de modo não autorizado ou não esperado;

Ataques externos: ocorrem quando usuários externos ou pessoas não autorizadas conseguem uma conexão externa e realizam acções inesperadas;

Armadilhas (*Trapdoor*): ocorrem quando um activo do sistema é modificado para produzir efeitos não autorizados em resposta a um comando ou a um evento premeditado;

Vírus/*Worms*: Um vírus de computador é um programa pequeno desenvolvido para alterar a forma como um computador opera, sem a permissão ou o conhecimento do seu usuário. Um vírus para se disseminar precisa de uma acção do homem, como por exemplo introduzir uma disquete infectada no computador. Enquanto que os ***worms***, de uma forma genérica, são uma espécie de vírus que devido a sua forma de reprodução, são considerados os mais desastrosos. E pela sua definição, são também programas capazes de se reproduzirem de um computador para o outro, porém sem a intervenção do homem;

Cavalos de Tróia (*trojan horse*): é um programa que se aloca como um arquivo no computador da vítima, com o intuito de roubar informações como identificação, *passwords e* números de cartões de crédito. Quando o computador contaminado por um *trojan* conecta-se à Internet, o intruso pode visualizar e capturar as informações digitadas pelo teclado ou contidas no disco duro do computador (SELEGUIM, 2003);

Backdoors - São portas[2] abertas de programas que facilitam a entrada dos atacantes no computador da vítima. Esta abertura pode ser acidental, como por exemplo, uma falha na fabricação de um programa ou proposital, quando esta porta é criada por um cavalo de tróia.

Escuta do trafego - Devido ao facto dos pacotes das aplicações que usam o modelo TCP/IP não serem criptografadas, é possível instalar em um determinado ponto da rede um programa chamado *Sniffer* que permite monitorar passivamente o trafego de redes. Os intrusos exploram esta facilidade para roubar a identificação e *passwords* de usuários e capturar números de cartões de crédito.

Para a realização de uma escuta do trafego da rede, basta ser instalado o *sniffer* em um ponto da rede por onde passa o trafego da informação.

Erro humano: O factor humano, segundo muitas pesquisas, tem se mostrado uma das fontes mais comuns de incidentes de segurança. Muitas vezes funcionários com acesso autorizado, porém desatentos e com pouco treinamento, podem tornar-se causa potencial de incidentes segurança (MACHADO, 2002).

---

[2] Portas são canais pelos quais são estabelecidas as comunicações/transmissões de dados de computador para computador, seja ela dentro de uma rede ou em uma comunicação externa.

E-mail - Existem vários riscos quando o assunto é *e-mail*, desde falsificação, roubo da informação, *spam*[3] até contaminação de uma rede por vírus. O e-mail apesar de ser um meio eficiente para a comunicação, ultimamente têm surgido diversas formas de burlar e torná-lo um meio de propagar vírus pela Internet.

2.3 MECANISMOS DE SEGURANÇA

Uma política de segurança e serviços de segurança[4] podem ser implementados através de vários mecanismos de segurança entre eles:

2.3.1 Autenticação

Em uma organização existem algumas pessoas que lidam com informações importantes que são restringidas ao restante dos funcionários, cabendo apenas as pessoas autorizadas o seu acesso. E para garantir que a pessoa que vai aceder os dados é realmente aquela que está autorizada, utiliza-se mecanismos de autenticação.

Estes mecanismos dividem-se em três tipos básicos: a autenticação baseada no nome e senha; cartões/certificados digitais; e impressão digital, análise de retina e reconhecimento de voz e da face, etc.

Para oferecer maior segurança é necessário que se aglutine mais de um tipo, como por exemplo, o cartão associado com nome e senha.

2.3.2 Senha

A senha tem uma importância muito grande para a salvaguarda da informação, pois é ela que garante o princípio da confidencialidade na segurança da informação.

Porém para estabelecer o seu uso adequado, deve ser definida uma série de recomendações que torne a senha forte e devem ser difundidas para todos os funcionários da organização.

2.3.3 Controlo de Acesso

Um dos grandes objectivos do controle de acesso é restringir o acesso não autorizado, principalmente daqueles que possam acarretar danos aos activos da organização.

Existem várias formas de garantir o controle de acesso para proteger a informação e o equipamento, por exemplo, o controlo do acesso à informação pelo sistema que a hospeda e o controlo do acesso

[3] O *spam* são mensagens não solicitadas, enviadas por e-mail pelo spammer (autor do *spam*), com o objectivo de apenas encher de "lixo" a caixa de entrada de mensagens. As vezes o *spam* é usado para publicidade.
[4] Os services de segurança em uma rede de computadores tem como função garantir a confidencialidade, integridade dos dados e autenticação das partes envolvidas.

físico de pessoas as áreas restritas; utilizando crachá, dispositivos biométricos, cartão magnético como forma de controle e se possível ter um monitoramento através de câmaras de vídeo.

2.3.4 Ferramentas para detectar vulnerabilidades

Existem várias ferramentas que permite detectar as vulnerabilidade internas e externa numa rede. Por exemplo o *scanner de vulnerabilidades RLINUX*, simula tentativas de acesso e ataques originados na rede interna e externa, testando assim todas vulnerabilidades no ambiente. Depois produz relatórios gráficos dos problemas de segurança encontrados, sem comprometer o funcionamento da rede. Nos relatórios são apresentadas alternativas para resolução dos problemas relacionados com as vulnerabilidades encontradas[5].

2.3.5 Criptografia

A criptografia é a arte ou a ciência de escrever em cifra ou em código, de forma a permitir que somente o destinatário decifre e compreenda a mensagem (VELOSO, 2002).

A criptografia é um dos princípios básicos da segurança da informação, pois ela protege as informações quanto a perda da confidencialidade.

Segundo CARVALHO (2003), com o passar dos tempos muitos métodos foram utilizados para cifrar e decifrar as mensagens, porém actualmente os métodos ficaram estabelecidos em criptografia simétrica (criptografia de chave privada) e criptografia assimétrica (criptografia de chave pública) que usam chaves para cifrar a informação.

As chaves são sequências de caracteres que são convertidos em *bits* e elas, através dos algoritmos de criptografia, são utilizadas na encriptação e desencriptação das mensagens. Os algoritmos de criptografia são funções matemáticas usadas para codificar os dados e a chave, porém são as chaves que garantem a segurança.

2.3.5.1 Criptografia por chave privada

A criptografia por chave privada baseia-se no utilização dos algoritmos simétricos que utilizam a mesma chave tanto para cifrar como para decifrar a informação. Pela sua característica no uso da chave, os algoritmos simétricos exigem que a chave seja mantida secreta e do conhecimento exclusivo dos dois interlocutores. Este facto dificulta a utilização destes algoritmos isoladamente. No entanto, é requerido um ***canal seguro*** que permita a um usuário enviar a chave ao seu interlocutor.

[5]RLINUX SOLUTIONS. http://www.rlinux.com.br/modules.php?name=Content&pa=showpage&pid=2 (28 Jun 2005)

O sistema criptográfico mais conhecido baseado em chave privada em uso actualmente é o *Data Encryption Standard* (DES) (VELOSO 2002).

2.3.5.2 Criptografia por chave pública

A Criptografia por chave pública baseia-se na utilização dos algoritmos assimétricos que usam um par de chaves distintas relacionadas (chave privada e chave pública), uma utilizada para cifrar e a outra para decifrar a informação.

Qualquer um dos possuidores da chave pública pode usá-la para cifrar uma mensagem. Porém a mesma mensagem só pode ser lida mediante o uso da chave privada correspondente que é de uso restrito pelo seu proprietário.

O único requisito deste sistema é que a chave pública esteja associada aos seus usuários de forma autenticável. Isto é, quando o emissor pretende enviar uma mensagem usando a chave pública, deve primeiro autenticar-se pela sua chave secreta.

Segundo VELOSO (2002), o sistema criptográfico mais conhecido de chaves assimétricas é o Rivest, Shamir and Adleman (RSA), o algoritmo de assinatura digital, *Digital Signature Algorithm* (DSA) é também um outro exemplo de técnica de chave publica utilizada para a assinatura digital de documentos electrónicos.

Este sistema possui duas aplicações principais: encriptação e assinatura digital.

2.3.6 Certificados Digitais

A criptografia por chave pública pode deixar a impressão que a segurança pode ser obtida de uma maneira simples. Um usuário distribui a sua chave pública e não tem a necessidade de nenhum outro controle para receber mensagens seguras. Entretanto, surgem os seguintes problemas:

- quem efectivamente está do outro lado da comunicação?
- a chave pública é realmente do usuário remoto desejado?
- a chave é ainda válida?

Estas questões segundo GOLDANI (2000), mostram que a criptografia por chave pública resolve efectivamente o problema da confidencialidade da informação transmitida mas não atende aos requisitos de integridade, autenticidade e deixa incertezas sobre a obtenção, reconhecimento, revogação, distribuição, validade e, mais importante, a vinculação da chave com uma entidade real.

As comunicações não podem ser verificadas em relação à autenticidade da origem (mensagem foi enviada pela origem declarada) e em relação à integridade dos dados (mensagem alterada em

trânsito), no entanto, as comunicações realizadas neste contexto podem ser privadas mas não são seguras.

Para atender aos requisitos de integridade e autenticidade foram implementados os Certificados Digitais que se baseiam na criptografia por chave pública, gerando um documento assinado digitalmente.

Os certificados digitais proporcionam uma vinculação entre a chave pública e algum atributo (como nome ou a identidade real) da entidade e administram todas as questões relacionadas anteriormente como a obtenção, reconhecimento, revogação, distribuição, validação e chave está vinculada a uma entidade do mundo real (GOLDANI, 2000).

Na primeira etapa do processo é assinado digitalmente o documento, aplicando a chave privada que é posteriormente enviado ao destinatário.

Na segunda etapa do processo, o receptor recebe a mensagem ou arquivo - o documento original + assinatura - que é decifrado usando a chave pública do remetente.

Por exemplo, segundo XEXÉO (?), o remetente para assinar uma mensagem, realiza um algoritmo envolvendo simultaneamente sua chave secreta e a mensagem propriamente dita, enviando o resultado, i.e., a assinatura junto com a mensagem (figura 2-1).

O destinatário, para verificar a assinatura, realiza um segundo algoritmo envolvendo a mensagem recebida, a assinatura e a chave publica do remetente. Se o resultado do algoritmo aplicado pelo destinatário for bem sucedido (figura 2-2), então a mensagem é considerada genuína, caso contrario, é considerada suspeita.

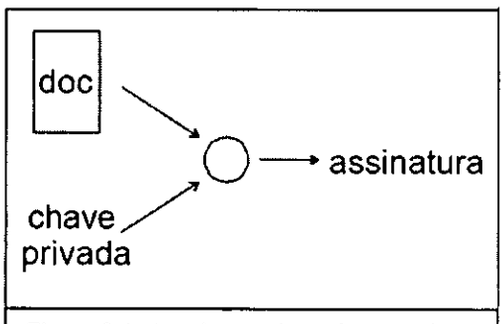


Figura 2-1: A assinatura é gerada por meio de uma função que tem como parâmetro a chave privada e o documento (XEXÉO, ?).

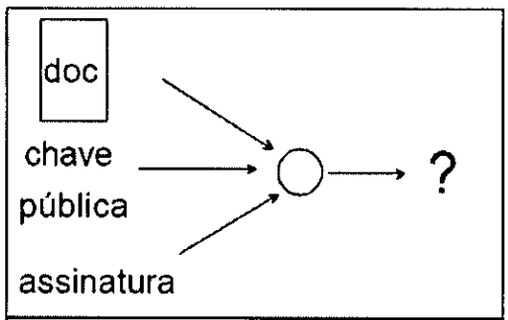


Figura 2-2: A verificação tem como parâmetros a chave publica, o documento e assinatura (XEXÉO, ?).

Os certificados apresentam atributos antifraudes que podem ser utilizados como referência para auxiliar quem recebe uma mensagem a decidir se o texto, a chave são confiáveis, sem consultar o remetente.

A veracidade dos dados contidos no certificado digital é assegurada pela entidade que o emitiu - a Autoridade Certificadora.

2.3.7 Backup

Backup é uma cópia de segurança da informação. O procedimento de backup é um cuidado muito importante para salvaguardar as informações contra qualquer tipo de ameaça, seja ela natural ou não.

Porém alguns cuidados devem ser tomados para garantir que o backup tenha sucesso, tais como: o local onde ficará guardado o backup deverá ser de acesso restrito; estar protegido contra poeira, calor, humidade e a prova de fogo; o local deverá ser fora da organização, de modo que caso ocorra um desastre na mesma não perderá os dados.

Para ter uma garantia maior é recomendado criptografar o *backup*; e deverá ter uma periodicidade na actualização, podendo ser de forma automatizada.

2.3.8 Firewall

O Firewall é um *software* que servem para filtrar pacotes através de regras estabelecidas, que podem ser configuradas ou ser padronizadas pelo fabricante do software. Constitui a barreira de protecção que separa a rede local da rede externa (Internet), sendo a primeira linha de defesa de uma rede, geralmente fica localizado entre o roteador e a rede interna.

Existem basicamente dois tipos de *firewalls*, que se diferem pela forma de bloqueio do tráfego, pois um é baseado em filtro de pacotes e o outro é baseado no bloqueio ou permissão de aplicações.

2.3.9 Sistemas de Detecção de Intrusão

O Sistemas de Detecção de Intrusão, (*Intrusion Detection System* (IDS)) é uma ferramenta cuja finalidade é detectar uma tentativa de invasão em tempo real que esteja ocorrendo dentro da rede. Ela pode somente alertar as tentativas de invasão, como também, aplicar medidas correctivas contra o ataque. Ou seja, podem actuar de modo passivo, apenas monitorando e analisando os tráfegos de uma rede, como também, de modo activo, onde uma vez reportado um ataque ele pode, como resposta, enviar um *e-mail* para o administrador ou emitir um sinal de alerta e encerrar as conexões entre atacante e o computador atacada.

2.4 POLÍTICA DE SEGURANÇA

A Política de Segurança é um conjunto de directrizes idealizadas pelos representantes de uma organização, moldadas de acordo com a funcionalidade da mesma, visando implementar a forma mais segura de utilizar a informação e os recursos computacionais.

A Política de Segurança procura estabelecer várias premissas, tais como: regras para o uso de determinados equipamentos, responsabilidades de cada membro da empresa, padronização de procedimentos, metas de segurança, treinamento para os usuários dos meios de informática, controle do acesso a informações, prevenção e detecção de vários tipos de ameaças, comprometimento da alta direcção e de seus funcionários, periodicidade de auditorias e avaliação de riscos, consciencialização dos usuários de informática, etc.

A política de segurança deve ser objectiva, simples, curta, verdadeira, válida para todos e ter o patrocínio da alta direcção da organização

2.5 AVALIAÇÃO DO RISCO

Segundo MAIA (2005), a Segurança da Informação não pode ser tratada somente na camada tecnológica. Existem outros elementos que são fundamentais e que devem ser considerados. Desta forma, em primeiro lugar devemos seleccionar um escopo para análise de riscos que contemple a tecnologia, o ambiente físico, as pessoas e os processos. Cada activo seleccionado no escopo deve estar enquadrado em uma dessas categorias.

Estes activos devem estar de acordo com as melhores práticas de segurança reconhecidas internacionalmente que são recomendações de segurança e padrões existentes, como por exemplo, a ISO 17799.

Segundo SYMANTEC (2004), uma empresa que segue o padrão ISO 17799 pode fazer mais negócios do que aquelas que não seguem um padrão. Se um cliente em potencial estiver escolhendo entre dois serviços diferentes, e a segurança for uma preocupação, ele geralmente seleccionará aquela que seguir determinado padrão na área. Além disso, uma empresa que segue o padrão ISO 17799 oferecerá segurança corporativa aprimorada, planeamento e gestão de segurança mais efectivo.

2.6 PLANO DE CONTIGÊNCIA

O Plano de Contingência também designado **plano de continuidade** ou **plano de desastre**, consiste em procedimentos de recuperação preestabelecidos, com a finalidade de minimizar o impacto sobre

as actividades da organização, no caso de ocorrência de um dano ou desastre que os procedimentos de segurança não conseguem evitar.

Tem como objectivo, dar a providência imediata invocando os procedimentos de recuperação dos sistemas corporativos, considerando o tempo de espera previsto para o restabelecimento da actividade.

O RFC 2196[6] é um guia que provê as recomendações básicas para elaboração de um Plano de contingência e planeamento da segurança de um site.

2.7 SEGURANÇA DO SITE

Segundo RFC 2196, a segurança do site diz respeito à protecção dos recursos computacionais presentes em uma rede privada. Tais recursos são compostos por *hosts* (computadores), roteadores, impressoras, informações armazenadas e software em geral.

O RFC 2196 provê as recomendações básicos sobre o planeamento de site seguro. Os principais passos a seguir são:

- Identificar o que proteger;
- Determinar de quem se proteger;
- Determinar quais são os tipos de ameaças.
- Definir e implementar medidas que irão proteger seus recursos de uma maneira efectiva.
- Rever todo o processo continuamente adaptando-o cada vez que uma nova vulnerabilidade for encontrada.

Para evitar falhas que possam causar a quebra da segurança é necessário prestar-se particular atenção ao factor humano, pois o sucesso ou falha do sistema de segurança montado depende da atitude do ser humano no exercício das suas actividades diárias. Também deve ser evitada a utilização de software de origem duvidosa porque pode apresentar falhas ou vulnerabilidades que podem ser exploradas por atacantes.

2.8 SEGURANÇA NAS COMUNICAÇÕES

A segurança nas comunicações trata da protecção da informação que está em circulação no meio de transmissão de dados.

O protocolo TCP/IP é inseguro, os pacotes que circulam através deste protocolo podem ser capturados por um indivíduo, não importando se são destinados a ele (GOLDANI 2001). Por esta

[6] **Site Security HandBook**. http://www.faqs.org/rfcs/rfc2196.html (19 Mai 2005)

razão, diversos mecanismos devem ser aplicados em conjunto para conferir maior segurança a informação durante a sua transmissão.

Com o objectivo de se obter um alto nível de segurança nas comunicações foram concebidos novos protocolos como o IPSec, SET, SSL, HTTPS e SSH, descritos a seguir.

2.8.1 *IP Security*

O *IP Security* (IPSec) é um padrão de protocolos criptográficos desenvolvidos para a nova versão do Protocolo da Internet (IPV6), para garantir uma comunicação segura entre computadores.

O IPSec é composto por três mecanismos criptográficos: *Authentication Header* (define a função *hashing* para assinatura digital); *Encapsulation Security Payload* (define o algoritmo simétrico para a encriptação) e ISAKMP (define o algoritmo assimétrico para a gestão e troca de chaves de criptografia)[7].

Com uso do IPSec e das tecnologias associadas, os dois computadores são capazes de se autenticar mutuamente e manter uma comunicação segura, com dados criptografados.

2.8.2 Secure Electronic Transaction

O Secure Electronic Transaction (SET) foi desenvolvido pela IBM em parceria com outras empresas, é aplicado no comércio electrónico em que existem três partes envolvidas na transacção: o cliente, o comerciante e o banco onde será efectuado o pagamento.

Esta comunicação triangular entre o cliente, o comerciante e o banco usando chaves de uso único, isto é destinadas para uma aplicação específica, e certificados digitais dá garantias as partes envolvidas e defesa da privacidade.

2.8.3 Secure Socket Layer

O Secure Socket Layer (SSL) é um protocolo desenvolvido pela Netscape Communications para transferir informações de modo seguro na Internet (HTTPS), desde que o servidor e o cliente utilizem este protocolo.

O SSL providencia autenticação, confidencialidade e integridade dos dados, sendo planeado para autenticar o servidor e opcionalmente o cliente. O SSL permite que o cliente se conecte ao *website*, de forma transparente é criado um canal de comunicação seguro entre o site e o cliente. Uma vez que esta conexão é estabelecida, informações, como o número de cartões de crédito, senhas de contas corrente, poderão ser fornecidas de uma maneira segura.

[7] http://training.com.br/lpmaia/pub_seg_cripto.htm (27 Mar 2005)

2.8.4 Hypertext Transport Protocol Secure

O protocolo padrão utilizado na Internet para transferir e exibir a informação é o HTTP (*Hypertext Transfer Protocol*) que é um protocolo aberto e que transmite as informações pela rede em texto claro, isto é, sem ser criptografado. Com o advento do *sniffer* este protocolo tornou-se inseguro pois as informações como senhas, nº de cartões de crédito podem ser interceptadas e lidas pelos intrusos.

Para prover maior segurança nas transações pela Internet o protocolo HTTP foi melhorado criando-se o protocolo *Hypertext Transport Protocol Secure* (HTTPS) que é um protocolo TCP/IP utilizado por servidores da *World Wide Web* e navegadores da Web para transferir e exibir páginas web e documentos de um modo seguro através da Internet. O HTTPS permite a encriptação e transmissão de informações através de uma porta especial.

Os serviços HTTPS pode ser implementados com a aplicados dos certificados digitais para a autenticação dos usuários pelo servidor web.

2.8.5 *Secure Shell*

O *Secure Shell* (SSH) é usado para aceder de forma segura uma máquina remota, com validação da máquina e encriptação de dados. O SSH foi criado para solucionar o problema da escuta do trafego com uma transferência de dados criptografada.

Os métodos de autenticação seleccionáveis incluem .rhosts apenas (inseguro) e .rhosts com validação do *host* através de RSA ou validação exclusiva através de RSA (PAULINO, 2003).

O exemplo mais simples de utilização de uma escuta é para capturar a senha de alguém que esteja fazendo telnet. A senha é passada entre a maquina cliente e o servidor de telnet como texto claro.

A autenticação das maquinas que se conectam remotamente é garantida pelo seu endereço IP ou pelo seu nome de domínio. Segundo PAULINO (2003), existem muitos métodos de falsificação de identidade IP, uma vez capturada a senha, o intruso é capaz de instalar uma escuta na rede e simular que é uma maquina autorizada, acedendo desta forma a máquina.

2.9 Conclusão

Não se pode falar, agir ou trabalhar com segurança sem antes estabelecer normas, padrões e directrizes de como usar as informações de maneira válida e segura. Um dos instrumentos fundamentais para estabelecer as directrizes de como manipular a informação e recursos de forma segura numa organização é a política de segurança da informação e dos recursos computacionais.

As pessoas representam o maior activo da organização, o sucesso ou falha da segurança dependerá da execução correcta do seu trabalho no dia a dia. Por isso, devem ser realizados programas contínuos de formação e de consciencialização que permitirão fortalecer a confiança e lealdade dos empregados.

Para garantir a segurança da rede de computadores é necessário tomar um conjunto de medidas e actualizá-las permanentemente com vista a minimizar as vulnerabilidades do sistema. Por exemplo, a actualização do Anti-vírus, aplicação dos *patches*[8] dos problemas conhecidos, utilização *do IDS e firewall,* para além da criptografia de chave pública associada aos certificados digitais que se revelam ser muito úteis para assinar os documentos e o correio electrónico, garantindo a sua autenticidade, integridade, confidencialidade e validade jurídica.

Os novos protocolos criados como o IPSec, SET, SSL, HTTPS e SSH com vista a promover o nível de segurança nas comunicações baseiam-se na utilização de certificados digitais.

Os certificados digitais, a criptografia de chave pública, as Autoridades Certificadoras com os protocolos e tecnologias associadas aos certificados digitais, constituem uma arquitectura de segurança de redes que, segundo SELEGUIM (2003), confere confiabilidade às transações electrónicas e tende assumir a condição de padrão mundial de autenticação de documentos e operações electrónicas.

Esta arquitectura é denominada *Infra-estrutura de Chave Pública* que confere maior segurança de uma maneira difícil de ser fraudada e que se apresenta de forma transparente para o usuário.

[8] Correcções ou actualizações de *software* disponibilizadas pelos seus fabricantes.

3. INFRA-ESTRUTURA DE CHAVE PÚBLICA

3.1 Introdução

A Infra-estrutura de Chave Pública (*Public Key Infrastructure* (PKI)) é uma combinação de hardware, software, tecnologias de encriptação, políticas e procedimentos necessários para criar, gerir, armazenar, distribuir e revogar certificados digitais (BARBOSA, 2005).

O objectivo desta arquitectura de segurança é distribuir a informação que é necessária em ambientes distribuídos, onde usuários e recursos estão em lugares diferentes, permitindo digitalmente a protecção da informação e a identificação segura dos interlocutores.

Em uma PKI o objecto central é o certificado digital (vide 3.10). Em torno dele gira um sistema complexo, composto por software e por procedimentos operacionais, integrando a criptografia de chave pública e autoridades de certificação numa arquitectura de segurança de redes completa para criar uma estrutura de confiança para os dois lados envolvidos nas transações electrónicas (SILVA, 2004).

A PKI associa as chaves públicas com as suas entidades, usando os certificados digitais, possibilitando que outras entidades verifiquem a validade das chaves públicas e disponibiliza os serviços necessários para a gestão das chaves que circulam pela rede.

Segundo MARTINS (2004), o funcionamento real de uma PKI, assim como a definição do número e das funções das entidades participantes depende intimamente de algumas decisões tomadas durante as fases de projecto da arquitectura do sistema.

Em transações comerciais convencionais, por exemplo, os clientes, os comerciantes e os bancos baseiam-se em certificados digitais para a identificação das partes e utilizam os cartões de crédito MasterCard ou VISA para completar a transação financeira.

A figura 3-1 apresenta a comunicação de dados entre as partes envolvidas numa transação do comércio electrónico.

1. Envio do pedido
    1.1 O Cliente envia o pedido ao Comerciante com a informação referente aos produtos e valor da compra e
    1.2 O Cliente envia o pedido ao Banco com informações do cartão, Comerciante e o valor a ser pago;
2. O Banco verifica os certificados digitais do Cliente e do Comerciante
3. O Banco envia a confirmação do pedido para o Comerciante;

4. Requisição do pagamento feita pelo Comerciante ao Banco;
5. O Banco processa o pagamento ao Comerciante;
6. Confirmação da entrega por e-mail.

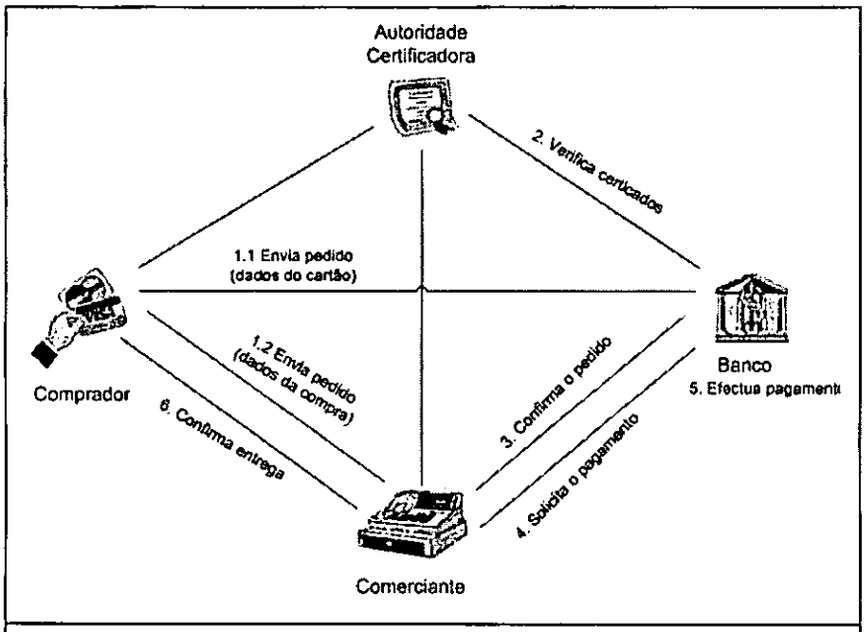


Figura 3-1: Esquema de compra electrónica (TORRES , ?)

Na comunicação triangular entre o Cliente, o Comerciante e o Banco usam chaves de uso único, isto é chaves para uso específico, e validade limitada, garantindo ao Comerciante que ele será pago, e ao Cliente que o Comerciante não poderá negar ter sido pago, e que o Banco não saberá o que o cliente está comprando (defesa da privacidade). A troca de mensagens relacionadas ao pagamento da compra é criptografada e enviada através do protocolo SET.

O presente capítulo apresenta uma abordagem detalhada sobre os componentes e padrões necessários para o estabelecimento e funcionamento de uma PKI.

3.2 Serviços disponibilizados com a utilização da PKI

A PKI oferece seis tipos de serviços básicos que permitem a realização de transacções electrónicas de forma segura:

- **Autenticidade da origem** - garante a identidade de quem envia a mensagem;
- **Controle de acesso** - os certificados são utilizados para associar um conjunto de atributos a uma entidade, permitindo deste modo restringir o acesso aos recursos;
- **Disponibilidade** - garante que a informação necessária para a realização de uma transação estará disponível para acesso no momento desejado;
- **Integridade** - garante que o conteúdo de uma mensagem não foi alterado;

- **Não-repudiação** - previne que alguém negue o envio e/ou recepção de uma mensagem;
- **Confidencialidade** - impede que pessoas não autorizadas tenham acesso ao conteúdo da mensagem, garantido que apenas a origem e o destino tenham conhecimento.

3.3 Arquitectura da PKI

A arquitectura genérica de uma PKI pode ser representada como ilustra a figura 3-2.

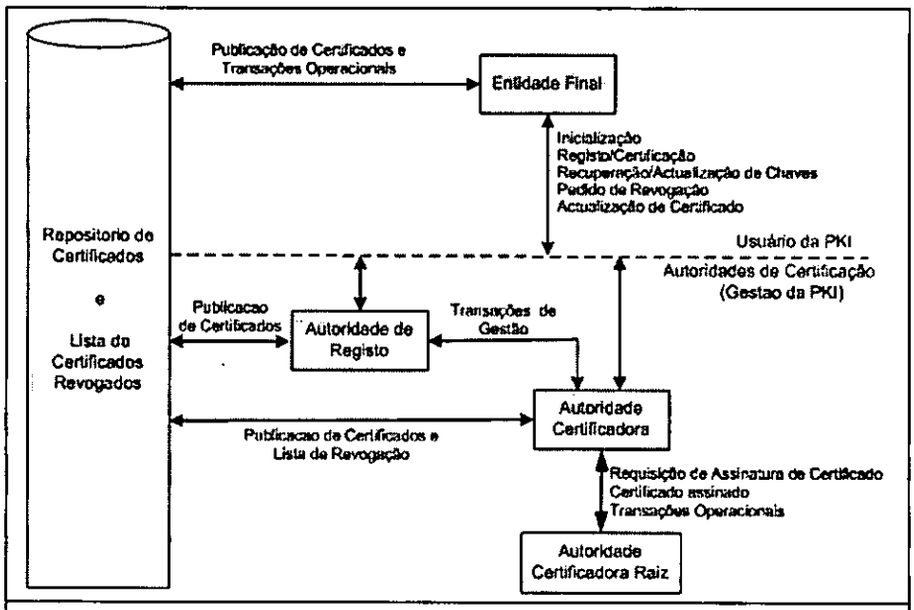


Figura 3-2: Arquitectura de uma PKI (XENITELLIS, 2000).

Alguns componentes na arquitectura de uma PKI podem ser desdobrados em uma ou mais entidades funcionais de acordo com as necessidades específicas do projecto.

Uma PKI é composta por três componentes: as autoridades de certificação, os clientes (entidades finais) e o repositório de certificados e Lista de Certificados Revogados.

3.3.1 Autoridades de certificação

As principais autoridades são: Autoridade Certificadora Raiz, Autoridade Certificadora e Autoridade de Registro. Em algumas implementações podem ser utilizadas outras autoridades com funções auxiliares.

3.3.1.1 Autoridade Certificadora Raiz

Autoridade Certificadora Raiz (AC-Raiz) é a primeira autoridade na cadeia de certificação, executa as políticas de certificação, as normas técnicas e operacionais. Também emite,

expede, distribui, revoga e gere os certificados e a Lista de Certificados Revogados (LCRs)[9]. das Autoridades Certificadoras do nível imediatamente subsequente ao seu.

A AC-Raiz executa actividades de fiscalização e auditoria das Autoridades Certificadoras, Autoridades de Registro e dos prestadores de serviços habilitados na PKI.

3.3.1.2 Autoridade Certificadora

A Autoridade Certificadora (AC) é a autoridade credenciada pela AC-Raiz para emitir certificados digitais para os usuários, vinculando pares de chaves criptográficas ao respectivo titular.

As ACs emitem, expedem, distribuem, revogam e gerem os certificados para os usuários, bem como colocam à sua disposição as LCRs e outras informações pertinentes e mantêm o registo de suas operações.

3.3.1.3 Autoridade de Registro

A Autoridade de Registro (AR) é uma entidade operacionalmente vinculada à AC, cujo as funções são: identificar e registrar os usuários presencialmente, encaminhar solicitações de certificados à AC e manter registros de suas operações.

A ideia da criação da AR é aliviar a carga da AC e partilhar as tarefas: a AR é responsável por validar o que está no certificado, e a AC pela sua emissão.

A presença da AR é opcional em ambientes pequenos.

Segundo MARTINS (2004), é importante que a transferência das informações necessárias à emissão de certificados da Autoridade de Registro para a AC não seja comprometida e que a segurança física da AC seja garantida (se a chave privada da AC tornar-se pública, todos os certificados assinados tornam-se inseguros).

3.3.2 Repositório de Certificados e Lista de Certificados Revogados

Segundo CARVALHO (2003), o repositório tem a função de armazenar e disponibilizar os certificados e a Lista de Certificados Revogados aos usuários da PKI a qualquer momento. Para isso, deve existir um tipo de repositório robusto, escalável e *on-line*.

Os repositórios são constituídos por directórios que são entradas unicamente identificadas, onde cada entrada possui um ou mais atributos com uma estrutura hierárquica de dados[10].

[9] São certificados declarados inválidos pela Autoridade de Certificação porque a entidade detentora de um certificado desiste de possuí-lo ou porque a Autoridade detectou uma violação.
[10] http://www.rnp.br/_arquivo/sci/2000/pki.pdf (29 Jun 2005)

Alguns exemplos de directórios são:

- Lista telefónica;
- Servidores de *Lightweight Directrory Acess Protocol* (LDAP);
- *Novel Directory Services* (NDS);
- *Windows Active Directory;*
- Agentes de Sistema de Directório X.500 (*Directory System Agents*);
- *Domain Name System* (DNS).

As relações destes três componentes constituem o modo de operação de uma PKI. Os padrões e protocolos interligam as relações necessárias, tornando a comunicação a mais padronizada possível de modo que produtos de empresas distintas possam se integrar.

3.3.3 Clientes

Os clientes são agrupados em duas classes, na figura 3-2 são indiscriminadamente representados como *entidade final*:

- **Titulares** de Certificados, que possuem certificados e utilizam na assinatura de documentos e
- **Clientes** que não possuem obrigatoriamente um certificado, utilizam a chave pública contida num certificado para cifrar mensagens e verificar assinaturas.

3.4 Hierarquia das Autoridades de Certificação

Uma PKI, assenta em hierarquias de confiança, a partir do momento em que se confia numa AC, confia-se em todos os certificados emitidos por ela.

Existem dois tipos básicos de estrutura das Autoridades Certificadoras, criadas para solucionar o problema de validação dos participantes em um processo de troca de informações: a estrutura Hierárquica e a Mista (SILVA, 2004).

3.4.1 Estrutura Hierárquica

A estrutura tradicional utilizada pela PKI é a Hierárquica. Nesta estrutura, múltiplas ACs prestam serviços de infra-estrutura e possuem uma relação de confiança de acordo com a sua hierárquica.

Nesta estrutura, todas as ACs confiam em uma AC central (AC-Raiz). Com a excepção da AC-Raiz, todas as outras ACs possuem uma única AC superior.

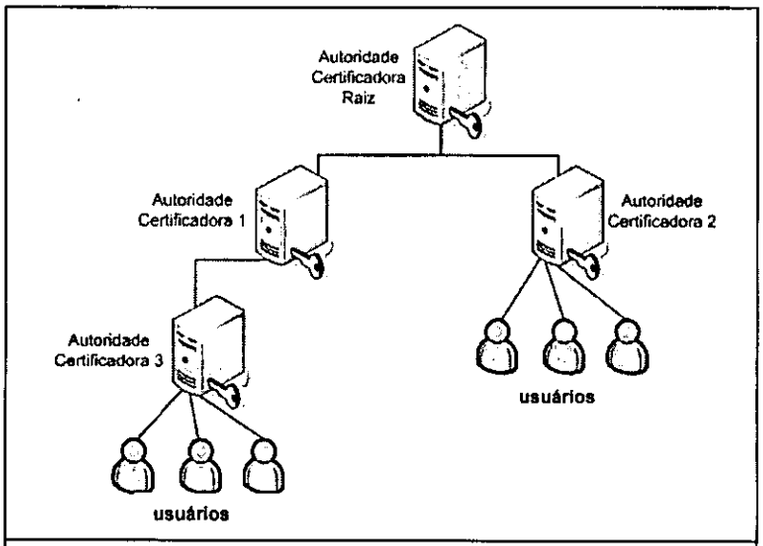


Figura 3-3: Estrutura hierárquica das Autoridades de Certificação (SILVA, 2004)

De acordo com SILVA (2004), a AC-Raiz é o topo da hierarquia, ou seja, o certificado digital da AC-Raiz é um certificado auto-assinado, pois ela não depende de nenhuma outra AC. Isto é necessário para garantir a validade da hierarquia das outras ACs. A partir daí, cada AC que for criada nessa estrutura terá seu certificado assinado pela AC-Raiz.

A AC 1 e AC 2 solicitam a assinatura de certificado a AC-Raiz e recebem desta seus certificados assinados pela chave secreta da AC-Raiz.

A AC 2 emite certificados digitais para usuários finais. A AC 1 emite apenas certificados para empresas ou outras ACs.

3.4.2 Estrutura Mista

Esta estrutura, também conhecida como **certificação cruzada**, múltiplas ACs se validam em um ambiente. Cada usuário confia em uma única AC, mas as ACs não se reportam unicamente a uma AC superior a ela, como acontece na arquitectura hierárquica. a AC-Raiz não é o último ponto desta rede. As ACs-Raiz podem confiar em outras ACs-Raiz, criando um ciclo de confiança e não limitando a sua abrangência apenas a sua hierarquia. A figura 3-4 apresenta um exemplo desta arquitectura.

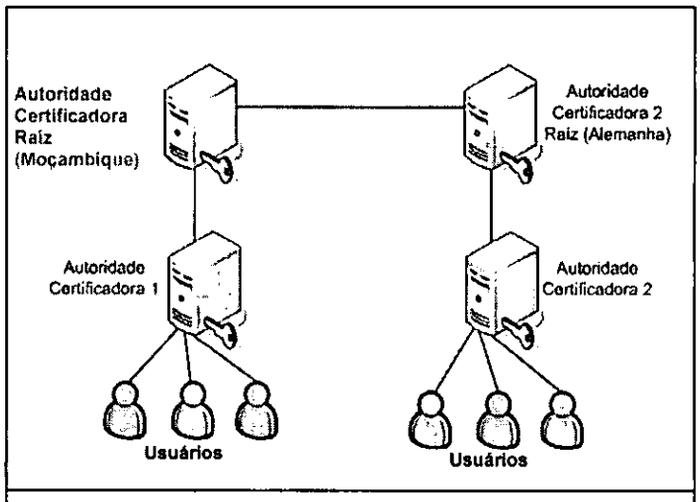


Figura 3-4: Estrutura Mista das Autoridades de Certificação (SILVA, 2004)

Neste caso se um cliente registado na AC moçambicana quiser realizar uma transação na Alemanha exibe um certificado situado abaixo da AC-Raiz de Moçambique. Quando for realizada na Alemanha a validação da cadeia de assinaturas irá perceber-se que aquele certificado não está abaixo na hierarquia da AC-Raiz da Alemanha. Mas a AC-Raiz da Alemanha possui confiança com a AC-Raiz de Moçambique por isso informará que o certificado em questão é válido e confiável. O cliente então poderá realizar a sua transacção.

De acordo com SILVA (2004), este procedimento é transparente para o cliente e esta arquitectura pode ser estabelecida com uma quantidade variável de ACs-Raiz.

3.5 Cadeias de Certificação e Confiança

Para utilizar um serviço que requeira o conhecimento de uma chave pública, é necessário obter e validar o certificado que a contenha.

A validação do certificado implica, por sua vez, o conhecimento da chave pública da Autoridade de Certificação que o emitiu e, consequentemente, a obtenção e validação do certificado que a contém.

A validação do certificado da AC poderá implicar o conhecimento da Chave Pública de outra AC que o tenha emitido, e assim sucessivamente. A sequência dos certificados entre a última AC subordinada e a AC-Raiz é chamada **Cadeia de Certificação** (GOLDANI, 2001).

A validação de uma cadeia de certificados terminará quando for encontrado o certificado procurado.

As cadeias de certificação reflectem uma hierarquia de Autoridades de Certificação.

3.6 Política de Certificado

Segundo BARBOSA (2005), uma Política de Certificado (*Certificate Policy*) é um conjunto de regras que define a aplicabilidade de certificados à uma determinada comunidade ou classe de aplicações.

A política deve compreender as seguintes questões: qual a legislação em que se baseará a emissão e utilização dos certificados; quais os requisitos e as responsabilidades associadas aos Titulares e Clientes; restrições de conteúdo e utilização dos certificados, p.e., apenas autenticação, somas máximas envolvidas numa transacção, etc. e os procedimentos a serem implementados relativamente a diversos aspectos do funcionamento de ACs e ARs.

O grau de confiança depositado numa AC depende da sua Política de Certificado e pode servir para ajudar um usuário a decidir quando é que um certificado é fidedigno o suficiente para ser usando em determinada aplicação.

3.7 Declaração de Práticas de Certificação

De acordo com o RFC 2527[11], uma Declaração de Práticas de Certificação (*Certification Practice Statement*) é um conjunto de regras que uma AC segue para emitir certificados. Tipicamente, apresenta as políticas para obtenção de vários níveis de certificados e o processo de registo que o usuário deve realizar para obter um certificado.

Segundo CARVALHO (2003), a Declaração de Práticas de Certificação tem informações mais detalhadas que a Política de Certificação. A Política de Certificado define os requisitos, enquanto que a Declaração de Práticas de Certificação explica como é que a PKI aplica os procedimentos para cumprir esses requisitos. Normalmente inclui também as definições de como a AC foi construída e opera, como os certificados são aceites, emitidos e revogados, como as chaves são geradas, registadas e certificadas, onde serão guardadas e como serão disponibilizadas aos usuários.

Ambas são disponibilizadas ao público através de uma extensão do certificado (vide 3.10.1), designada por "*certificate policies*".

3.8 Padrões Relacionados com PKI

Para garantir a interoperabilidade entre diferentes plataformas e não vinculação a soluções proprietárias, a PKI baseia-se em padrões e protocolos que tornam a comunicação consistente.

Segundo GOLDANI (2001), os padrões necessários para operacionalizar o ambiente PKI podem ser divididos em duas categorias:

[11] http://www.freeicp.org/twiki/bin/view/Docs/RequestForComments2527 (12 Abr 2005)

- Padrões que definem a PKI; e
- Padrões de segurança que necessitam da PKI.

A figura 3-5, mostra as relações entre os padrões que definem uma PKI e os padrões de segurança para aplicações que podem necessitar ou permitir o uso da PKI.

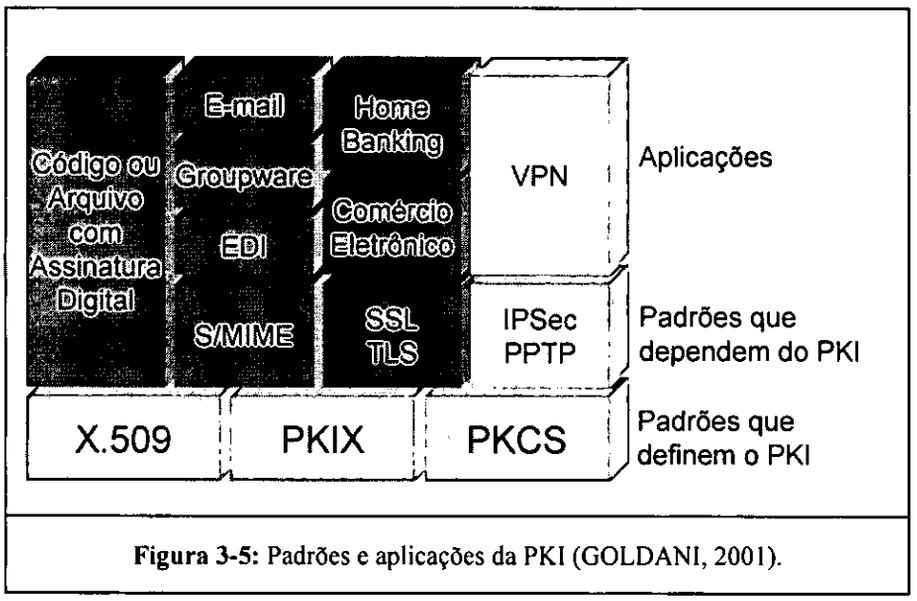


Figura 3-5: Padrões e aplicações da PKI (GOLDANI, 2001).

3.8.1 Padrões que definem a PKI

Os padrões são necessários para compatibilizar em múltiplas aplicações as operações como:

- Procedimentos de inicialização e troca de informações para o registo dos titulares;
- Formato de certificados;
- Formato de Lista de Certificados Revogados;
- Formato de assinaturas digitais;
- Recuperação e actualização de pares de chaves

3.8.1.1 X.509

A Recomendação X.509 possui dois formatos de certificação, um para gerar certificados digitais e outro para divulgar a Lista dos Certificados Revogados.

O padrão define duas estruturas para certificados: certificados de chave pública que associa a entidade-fim (*End Entity*) com a respectiva chave pública, chamado usualmente de certificado digital e outra estrutura, para certificados de atributos que são utilizados na autenticação baseada em regras de acesso e nas funções de seus usuários.

O certificado definido pela X.509 passou por duas versões, sendo a actual (X.509v3) composto por dez (10) campos básicos e extensões (vide 3.10.1). Segundo STANTON (2002), a principal função das extensões é permitir a inclusão de novos campos aos certificados, sem necessidade de modificação de sua estrutura de codificação, tais como: políticas de certificação; nomes alternativos de emissores e proprietários.

O X.509 aplica nas operações de registo, revogação e distribuição das Listas de Certificados Revogados os padrões de criptografia (vide 3.8.1.3).

3.8.1.2 PKIX

A *Internet X.509 Public Key Infrastructure* (PKIX) é uma especialização do padrão X.509 de certificados digitais, voltados para uso na Internet elaborado pela *Internet Engineering Task Force* (IETF) para prover funções de identificação, autenticação, controle de acesso e autorização de modo determinístico e automático na Internet. Seu desenvolvimento foi motivado pelo facto de que a X.509 definir uma estrutura muito genérica (GOLDANI, 2001).

Esta proposta de padronização define perfis e protocolos de certificados e LCRs, bem como impõe um número de restrições, projectadas para melhorar a gestão e a interoperabilidade de aplicações da PKI.

Embora a PKIX seja baseada na Recomendação X.509, ela não requer o uso de sistemas de directórios X.500 e permite o uso de outros métodos de distribuição de certificados e Lista de Certificados Revogados.

A PKIX define o formato e a semântica de certificados e Lista de Certificados Revogados para uso na Internet, para **propósitos específicos**, tais como correio electrónico, WWW e IPSec. Os campos básicos dos certificados são os mesmos definidos no padrão X.509, como também as suas extensões.

As especificações do PKIX são baseadas no padrão X.509 da União Internacional de Telecomunicações (ITU) e nos padrões de criptografia por chave pública (*Public Key Cryptography Standards*) da RSA *Security*.

3.8.1.3 *Public key Cryptography Standards*

Os *Public key Cryptography Standards* (PKCS) são padrões de criptografia utilizados na PKI nas áreas de registro, revogação e distribuição de Lista de Certificados Revogados. Segundo CARVALHO (2003), as três especificações mais importantes e mais utilizadas actualmente são o PKCS#7, PKCS#10 e PKCS#12 descritos na tabela 3-1.

Padrão	Descrição
PKCS#1	Define mecanismos para encriptação e assinatura de dados usando o sistema RSA
PKCS#3	Define o padrão de chaves Diffie-Hellman[12]
PKCS#5	Descreve um método para gerar uma chave secreta baseado em uma senha
PKCS#6	Padrão de sintaxe de certificado
PKCS#7	Define uma sintaxe genérica para mensagens que devem ser criptografadas
PKCS#8	Define um método para guarda de informações de chave privada
PKCS#9	Define tipos de atributos para uso nos protocolos PKCS
PKCS#10	Padrão de Requisição de Certificados
PKCS#11	Padrão de interface para criptografia em tokens
PKCS#12	Descreve um formato portátil para guarda e transporte de chaves privadas, certificados, etc.
PKCS#13	Define mecanismos para encriptação e assinatura de dados usando o algoritmo de curvas elípticas
PKCS#14	Padrão para geração de números pseudo-randômicos
PKCS#15	Descreve um padrão para informações credenciais criptografadas armazenadas em tokens

Tabela 3-1: Descrição dos padrões de criptografia (CARVALHO, 2003)

3.8.1.4 Protocolo X.500

A recomendação X.500 inclui em sua estrutura básica o seguinte:

- um conjunto de funções de directório referentes a operações de leitura e busca de dados armazenados;
- aspectos de segurança relacionados ao controle de acesso e à modificação da base de dados; e
- protocolos que definem a interacção de directórios e seus usuários, como também entre directórios distribuídos.

O protocolo utilizado pelos usuários para aceder o directório é chamado por *Directory Access Protocol* (DAP)[13].

LDAP

O *Lightweight Directory Access Protocol* (LDAP) é baseado no mesmo modelo de informação da X.500, foi definido com o intuito de remover algumas restrições daquela recomendação, permitindo que os serviços de directório fossem disponibilizados a maior variedade de máquinas e aplicações. O LDAP foi projectado para ser empregado directamente sobre a camada TCP/IP. Possui um modelo de dados flexível e tem sido usado como padrão entre vários fabricantes de *software*[14].

[12] Método Criptográfico de Chave pública/Chave privada, permite que dois utilizadores troquem uma chave de forma segura para cifrar/decifrar mensagens usando um canal de comunicação publico.

[13] http://www.rnp.br/newsgen/0203/processamento_dinamico.html#ng-2-1. (04 Mai 2005)

[14] http://www.rnp.br/_arquivo/sci/2000/pki.pdf. (29 Jun 2005)

3.8.2 Padrões que dependem da PKI

A maioria dos padrões de segurança para aplicações foram projectados para operar com PKI. O SSL (Secure Socket Layer), TLS (Transport Layer Security), Secure Multipurpose Internet Mail Extensions (S/MIME), Secure Electronic Transactions (SET) e IP security (IPSec) necessitam ou permitem o uso de PKI.

S/MIME: é um padrão IETF para a segurança de mensagens. O S/MIME pressupõe uma PKI para assinar mensagens digitalmente e criptografar mensagens e anexos.

SSL e TSL: são os padrões mais importantes para a segurança no acesso a servidores Web. Estes protocolos também são usados para prover segurança em ambientes cliente/servidor e em outras aplicações não Web. Ambos dependem de uma PKI para emissão de certificados para clientes e servidores.

SET: O *Secure Electronic Transaction* foi desenvolvido para facilitar os pagamentos bancários com cartões. O SET usa chaves para autenticação, confidencialidade e integridade de dados. O PKI é crítico como base para a autenticação das entidade envolvidas em uma transação de pagamentos.

IPSec: é um padrão IETF que define criptografia em IP e foi um dos primeiros protocolos utilizados no desenvolvimento de Redes Virtuais Privadas (VPNs – *Virtual Private Networks*). Segundo GOLDANI (2001), o padrão ainda está em desenvolvimento e a PKI é o modo mais apropriado (escalável) para administrar as chaves do IPSec. O uso do IPSec ainda é muito limitado, mas tende a crescer com o desenvolvimento do PKI.

3.9 Funcionamento da PKI

A componente tecnológica que constitui a PKI pode ser representada como ilustra a figura abaixo.

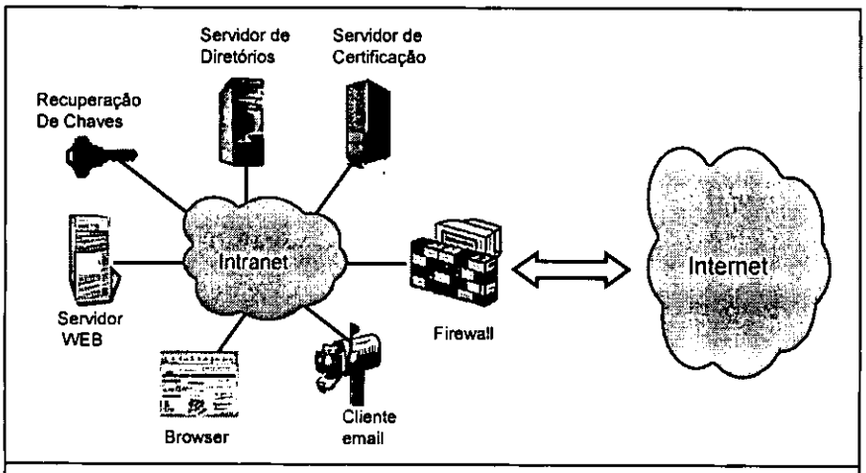


Figura 3-6: Infra-estrutura que compõe a PKI (GOLDANI, 2001*)

Os servidores da PKI são a Autoridade Certificadora (servidor de certificados), os directórios e sistemas de recuperação de chaves. Os clientes da PKI são o servidor Web, browser, e-mail e outras aplicações.

3.9.1 Servidor de Certificados

Um servidor de certificados emite, administra e revoga certificados digitais. A chave pública da AC tem credibilidade e é conhecido por todas as entidades participantes.

Para melhorar a performance (evitar congestionamento da rede) ou por razões de segurança (evitar que a falha de um único ponto comprometa todo o sistema) e facilitar a administração, a AC pode delegar a sua credibilidade para uma autoridade subordinada assinando o seu certificado e criando uma hierarquia de certificação.

3.9.2 Servidor de directórios

Os registos nos directórios podem incluir usuários, recursos da rede tais como servidores ou impressoras. O servidor de directórios fornece um único ponto de administração para as informações pessoais e corporativas.

As informações dos usuários como *e-mail*, endereço, telefone, privilégios e certificados podem ficar disponíveis para múltiplas aplicações de acordo com uma política de segurança definida. Os clientes de directórios podem localizar registros e atributos utilizando protocolos de acesso como, por exemplo, o LDAP que permite as aplicações com plataformas distintas possam ter acesso aos directórios.

3.9.3 Servidor para recuperação de chaves

Segundo **GOLDANI** (2001*), o servidor para recuperação de chaves permite que clientes armazenem e recuperem chaves de criptografia. Esta função é necessária para ter acesso a arquivos criptografados caso a chave privada seja danificada. Este servidor também pode ser utilizado como um tipo de procurador do usuário para permitir, na ausência deste, o acesso a informações de propriedade da empresa.

3.9.4 Armazenamento seguro de chaves

O elemento sensível desta infra-estrutura é a chave privada, quer seja de uma autoridade de certificação ou de usuários, devendo por isso ser protegida da melhor forma possível. Se for descoberta por terceiros, elimina a propriedade da autenticidade que esta garante. No caso da chave privada de AC, a situação é gravíssima pois destruirá toda a hierarquia de segurança nela suspensa (CARVALHO, 2003).

Assim, para além da sensibilização aos usuários quanto a cuidados que deve ter em consideração, utiliza-se dispositivos de armazenamento considerados robustos para a protecção da chave.

O armazenamento de chaves em disquetes ou em disco não é seguro, pois estes suportes são de fácil acesso, a chave pode ser eliminada ou copiada facilmente.

De seguida, apresenta-se três dispositivos de armazenamento de chaves considerados seguros e robustos:

3.9.4.1 Smart Card

Smart card é um cartão contendo um *chip* responsável pela geração e armazenamento de informações que dizem respeito ao usuário e certificados digitais.

Tem como principais características a resistência à alteração, o *chip* não é lido através de meios físicos directos, e a capacidade de detecção de ataques por raios ultravioleta.

Segundo CARVALHO (2003), o *smart card* tem a capacidade para gerar a chave privada dentro do cartão sendo guardada num ficheiro secreto. A chave pública é gerada fora do cartão sendo juntamente com o certificado associado guardada no cartão.

O *smart card* tem a vantagem de apresentar os dados do seu titular impressos na sua superfície, funcionando como um cartão de identificação. Como desvantagem apresenta o custo, uma vez que requer a aquisição do cartão e do respectivo leitor.

3.9.4.2 USB Token

O *USB Token*, possui as mesmas características lógicas e de segurança que um *smart card* (o seu conteúdo é protegido por PIN, guarda o par de chaves assimétricas, gera a chave privada, etc.), deferindo deste ao nível físico, conectado a qualquer computador através da porta USB.

O USB Token consiste em dois componentes de hardware: um controlador/chip criptográfico e um controlador USB.

É um hardware criptográfico que gera e armazena as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas essas chaves, elas estarão totalmente protegidas, não sendo possível exportá-las para uma outra mídia nem retirá-las.

3.9.4.3 *Hardware Security Module*

O Módulo de Segurança em Hardware é um dispositivo resistente a alterações, utilizado em sistemas criptográficos como um método que garante a segurança de uma variedade de operações.

Normalmente é o dispositivo utilizado para armazenar a chave privada da AC, desempenhando as seguintes funções:

- assinatura de certificados;
- geração de chaves para os usários; e
- geração das chaves da AC dentro do módulo.

O código de acesso ao seu conteúdo é feito através da combinação de fragmentos de uma chave simétrica guardados em vários *smart cards* distribuídos aos operadores da AC.

3.9.5 Clientes PKI

Segundo GOLDANI (2001*), todos os clientes PKI devem, no mínimo, estarem aptos a gerar assinaturas digitais e administrar certificados. Os requisitos das aplicações PKI são:

- Gerar pares de chaves pública/privada;
- Criar uma solicitação de certificados (PKCS#10);
- Apresentar e verificar um certificado;
- Excluir um certificado;
- Solicitar uma revogação de certificado;
- Armazenar certificados com critérios de segurança (exemplo: protecção por *password*);
- Exportar certificados com segurança (PKCS#12);
- Seleccionar algoritmos, resistência de chaves e controles de *passwords*;
- Configurar opções de segurança (por exemplo: assinar e criptografar sempre que possível).

3.9.6 Vantagens da PKI

A implementação de um PKI permite comunicações seguras em redes compartilhadas que é uma condição fundamental para a realização de transações electrónicas, com maior destaque para o comércio electrónico, oferecendo ainda:

- Excelente modularidade (escalabilidade);
- Mesma tecnologia para uma ampla variedade de aplicações;
- Centrada em padrões internacionais (interoperabilidade);
- Usuários que não se conhecem podem estabelecer comunicações seguras se existir uma "cadeia de credibilidade" de Autoridades Certificadoras (ACs);
- Reduz os problemas relacionados com distribuição de chaves;
- Não necessitam chaves pré-compartilhadas;
- Administra relações "vários para vários".

3.10 CERTIFICADOS DIGITAIS

A certificação digital tem origem através da necessidade crescente do mundo actual de transpor a mesma credibilidade e segurança existentes hoje no mundo do papel para o mundo digital (documentos e transações electrónicas). Essa necessidade é consolidada através da implementação da autenticação, integridade, confidencialidade e não-repudiação da informação.

Tecnologicamente, esses conceitos são implementados através dos sistemas de criptografia de chave pública, que são baseados na existência de um par de chaves relacionadas.

Um Certificado Digital é uma credencial electrónica que identifica pessoas físicas e jurídicas, sendo, portanto análogo a um documento de identidade digital ou um passaporte digital (MARTINS, 2004).

Segundo CARVALHO (2003), actualmente sempre que se faz referência a certificados digitais, é do certificado de chave pública X.509 que se está a falar, pois é o que está a ser usado pela maioria das aplicações.

Um Certificado garante a associação da chave pública a uma determinada entidade. A associação chave-entidade é estabelecida por uma terceira entidade, a Autoridade Certificadora, que assina digitalmente e gere o ciclo de vida dos certificados. Os certificados digitais permitem a autenticação do emissor da mensagem e criptografia dos dados, possibilitando o fluxo de informações confidenciais sobre meios de comunicação não seguros como a Internet.

A utilidade de um certificado depende unicamente da confiança depositada na Autoridade de Certificação, pois esta é que gere todo o processo de certificação.

Para transmitir a segurança e credibilidade da identidade digital, o certificado engloba diversas informações relevantes sobre o seu titular e também a sua chave pública.

Existem três modelos de certificados que são: X.509, *Pretty Good Privacy* e *Simple Public Key Infrastructure*.

O certificado X.509 é uma recomendação do ITU, descreve dois níveis de autenticação: **autenticação simples**, usando uma password para verificar uma identidade e **autenticação forte**, envolvendo credenciais consolidadas por técnicas criptográficas, utiliza uma estrutura de serviços baseada em directórios que são implementados pela AC.

Certificado "*Pretty Good Privacy*" (PGP), baseia-se no conceito de que as relações de confiança são feitas entre indivíduos, eliminando a existência de uma terceira parte confiante. Tal estrutura não interessa aos sistemas corporativos nos quais se pretende que as decisões de estabelecimentos de confiança sejam efectuados ao nível das organizações.

Certificado "*Simple Public Key Infrastructure*" (SPKI), é uma adaptação do padrão X.509 para a Internet, baseada na estrutura PKI, tornado mais simples e perceptível para a Internet. Por conseguinte, o certificado gerado por esta infra-estrutura seria também fácil de utilizar. No entanto, segundo CARVALHO (2003), após a sua conclusão, não houve grande procura no mercado pelo que o vendedores optaram por não investir nele.

Os três modelos administram os processos de modo diferente, o certificado X.509 é o mais aceite e utilizado num grande conjunto de aplicações como o S/MIME, IPSec, SSL e SET por isso merecerá particular atenção neste trabalho.

O modelo X.509 v3 possui várias classes de certificados como: certificado para usuários, certificados de atributos, certificados para servidores e a Lista de Certificados Revogados.

3.10.1 Certificados para usuários (Modelo X.509 v3)

O padrão X.509 faz parte de um conjunto de recomendações X.500 que definem um conjunto de serviço de directório. A estrutura deste certificado foi sendo melhorada encontrando-se actualmente na terceira versão (X.509 v3).

A figura 3.7, na página seguinte, mostra o guia *General* de um certificado digital que contém informações que indicam os propósitos para os quais foi emitido o certificado digital, o titular, o emissor e data de validade do certificado.

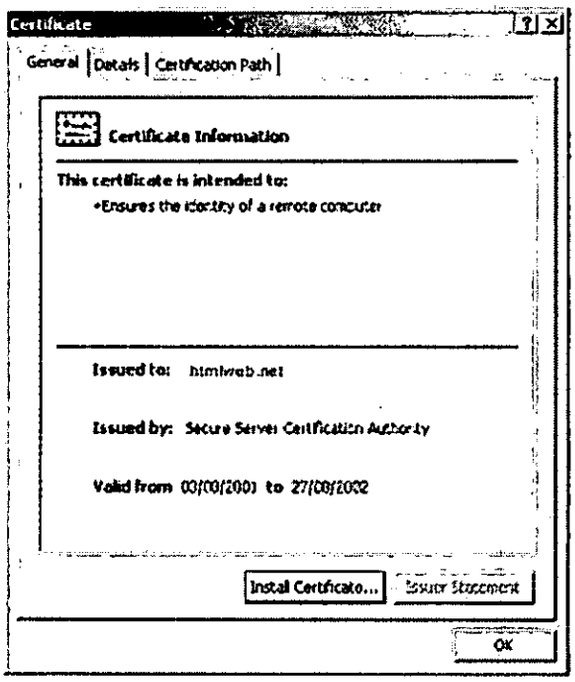


Figura 3-7: Certificado digital[15]

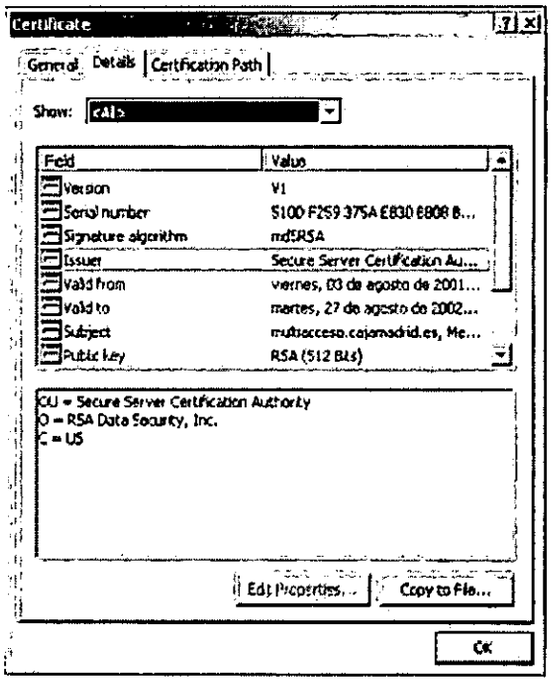


Figura 3-8: Campos de um certificado digital[16]

A figura 3-8, mostra o guia *Details* que contém os campos de um certificado.

O guia *Certification Path* contém a cadeia de certificação que é a hierarquia correcta desde a AC-Raiz até ao certificado do utilizador.

Campos de um certificado

A tabela a baixo representa a disposição dos campos contidos no guia *details* de um certificado do padrão X.509 v3.

Versão
Número da Série
Identificador do Algoritmo de Assinatura
Nome do Emissor
Período de Validade
Nome do Titular
Identificação da Chave Pública do Titular
Identificador Único do Emissor
Identificador Único do Titular
Extensões
Assinatura Digital

Tabela 3-2: Campos de um certificado digital

[15] http://www.htmlweb.net/seguridad/ssl/images/certificado_1.gif (14 Jun 2005)
[16] http://www.htmlweb.net/seguridad/ssl/images/certificado_2.gif (14 Jun 2005)

Versão - Identifica a versão do certificado X.509, a versão actual e 3;

Número da Série - este campo contém um identificador único do certificado, emitido pela correspondente AC;

Identificador do Algoritmo de Assinatura - Indica o algoritmo utilizado para assinar o certificado;

Nome do Emissor - Indica o nome distinto (*Distinguished Name* - DN) que é a identificação da AC que emitiu e assinou o certificado;

Período de Validade – Define o período de validade de um certificado, a menos que seja revogado;

Nome do Titular – Indica o DN da entidade final a que o certificado se refere;

Identificação da Chave Pública do Titular – Este campo possui a chave pública do titular e o identificador do algoritmo com o qual ela é utilizada;

Identificador Único do Emissor – Este campo é opcional, contém um identificador único para evitar ambiguidade no nome da AC, no caso em que o mesmo nome foi usado por diferentes entidades;

Identificador Único do Titular - Este campo é opcional, contém um identificador único para evitar ambiguidade no nome do proprietário do certificado;

Extensões – As extensões permitem tornar o certificado mais flexível e com um leque maior de utilização. As extensões são marcadas como *Critica*l ou *Non Critical*, uma aplicação que encontre uma extensão crítica que não reconheça tem de rejeitar o certificado. Entre outros aspectos, as extensões permitem a indicação das limitações à responsabilidade da AC e política de certificação.

As extensões mais utilizadas são:

Identificador de chave de autoridade - este campo é utilizado para diferenciar chaves de assinaturas com múltiplos certificados de uma mesma AC. A AC fornece um ponteiro para um outro certificado;

Identificador de chave do titular - este campo é utilizado para diferenciar chaves de assinaturas com múltiplos certificados do mesmo proprietário. O proprietário fornece um ponteiro para um outro certificado;

Utilização da chave - que limita o uso das chaves para determinados propósitos;

Ponto de distribuição da LCR - apresenta um identificador para localizar a estrutura de LCR definida;

Política de certificado - contém informações sobre as políticas e qualificadores opcionais que a AC associa ao certificado;

Nome alternativo do titular - indica uma ou mais formas alternativas de nomes associados ao proprietário desse certificado;

Nome alternativo do emissor - indica uma ou mais formas alternativas de nomes associados ao emissor do certificado.

Assinatura Digital - informação associada ao certificado para garantir a sua autenticidade.

3.10.2 Certificado de Atributos

Os certificados de chave pública associam uma identidade a uma chave pública. Os certificados de atributos constituem um caso mais genérico: associam um conjunto de atributos (permissões ou privilégios) a uma identidade (MARTINS, 2004).

O RFC 3281 da IETF é uma recomendação para a utilização deste tipo de certificados na Internet, definindo os atributos e extensões.

Os certificado de atributos são utilizados em aplicações de controlo de acesso a recursos, onde as autorizações (permissões e privilégios) são mais importantes do que a identidade.

3.10.3 Certificado Digital SSL

O Certificado Digital SSL (Servidor Seguro) oferece aos visitantes e clientes de um portal de serviços ou website uma plataforma de autenticação dos sites e confiança com maior segurança nas transações electrónicos realizadas[17].

O selo de segurança (cadeado que aparece na parte inferior do navegador nos sites que tem certificado para a sua autenticação) assegura aos clientes que os números dos cartões de crédito ou outras informações confidenciais não serão vistas, interceptadas ou alteradas, pois a comunicação entre o site e o cliente é toda criptografada e segura.

Figura 3-9: Selo de segurança de um site de Internet.

O Certificado SSL actualmente usado é o da chave de criptografia de 128 bits que é instalado na conta de hospedagem do site ou no servidor dedicado.

Se o nível de autenticação requerido no site for obrigatório, o site protegido exigirá um certificado à todos clientes.

[17] http://www.insidehost.com.br/soluções/servidor_ssl.php (28 Mai 2005)

O servidor valida os clientes verificando um certificado raiz das autoridades de certificação confiáveis no banco de dados de chave local. Os clientes validam o certificado do servidor verificando o certificado raiz das ACs instaladas no *browser*.

3.10.4 Lista de Certificados Revogados

A Lista de Certificados Revogados (LCRs) é um método de revogação definido pelo padrão X.509. Consiste numa estrutura de dados que contém a lista dos certificados cancelados. Esta estrutura é assinada digitalmente pela AC que emitiu esses certificados (CARVALHO, 2003).

A LCRs é um mecanismo de publicação periódica que disponibilizado no repositório. Tal como sucede com os certificados, a sua autenticidade e integridade são confirmadas pela assinatura ligada a essa LCRs. O local e o protocolo de acesso à lista é definido em um campo de extensão em cada certificado emitido.

A LCRs possui a vantagem de verificação on-line do estado do certificado, contudo, possui algumas limitações como por exemplo, se um pedido de revogação for efectuado neste preciso momento, tal revogação não será notificada aos usuários até a próxima actualização da LCRs.

Para reduzir a latência entre o aviso de pedido de revogação e o conhecimento desta pelos usuários, a alternativa é a aplicação do Protocolo de Estado do Certificado em modo On-line (*On-line Certificate Status Protocol (OCSP)*).

O usuário que tenciona saber o estado de determinado certificado, envia o pedido ao servidor de OCSP da AC, suspendendo a aceitação do certificado até que aquele lhe envie uma resposta.

3.10.5 Ciclo de Vida de um certificado digital

Segundo MARTINS (2004), um certificado uma vez emitido nunca mais deixa de existir, isto é, não se pode deliberadamente remover um certificado de um repositório devido a alguma falha na sua criação ou pela sua revogação. Isto ocorre porque o certificado em questão pode já estar sendo usado e a ausência do mesmo no repositório cria uma inconsistência, podendo gerar desconfiança sobre o processo de emissão.

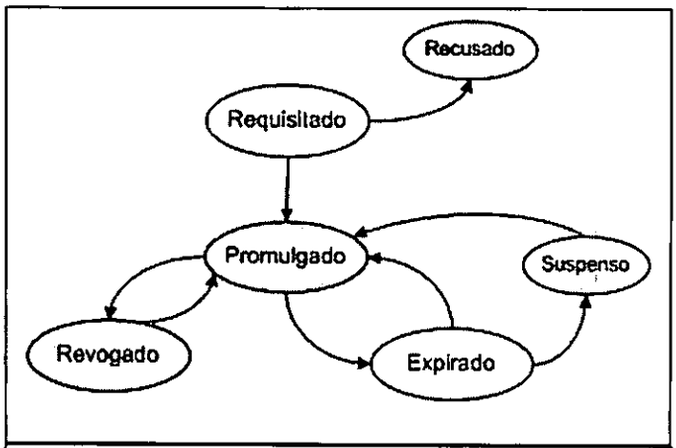


Figura 3-10: Estados que ilustram o ciclo de vida de um certificado digital

O ciclo de vida de um certificado digital inicia com a sua requisição pelo usuário (estado **requisitado**), sendo posteriormente

promulgado ou **recusado** pela AC. Se for promulgado quando ultrapassa o período de sua validade passa para o estado **expirado,** onde poderá ser re-assinado retornando ao estado promulgado, caso contrário ficará **suspenso**. O certificado permanecerá **suspenso** enquanto não for re-assinado, uma vez regularizado retornará ao estado **promulgado**. Durante o estado **promulgado** (dentro do período de validade) o certificado pode ser cancelado a pedido do seu titular ou se a AC detectar alguma irregularidade, passando deste modo para o estado **revogado**. O certificado pode retornar ao estado promulgado se for ultrapassada a irregularidade ou a pedido do seu titular.

3.11 ASSINATURA DIGITAL

A assinatura digital é um conjunto de procedimentos matemáticos realizados com a utilização de técnicas de criptografia que permite de forma única e exclusiva, a comprovação da autoria de um determinado conjunto de dados de computador (um arquivo, um e-mail ou uma transação)[18].

Uma assinatura digital é a informação que acompanha ou está associada à uma mensagem codificada digitalmente e que pode ser usada para garantir autenticidade, integridade e não-repudiação da mensagem enviada.

A finalidade da assinatura digital é garantir a integridade da informação, identificar o autor do documento e indicar a data e a hora da assinatura do documentos electrónico.

A assinatura digital é dinâmica por natureza pois é constituída pelo **resumo do documento a enviar**[19] e a **chave privada.** Por isso será única para cada mensagem ou documento assinado. Deste modo torna-se praticamente impossível a sua falsificação e comprova que a pessoa que a criou concorda com o documento assinado digitalmente, como a assinatura do próprio punho comprova a autoria de um documento escrito.

Os documentos em geral, para serem legalmente válidos, precisam possuir confiança e credibilidade que dependem de três características: a autenticação, integridade e não-repudiação. Para que seja autêntico, o documento não pode sofrer alterações, seja por erros humanos (involuntários ou intencionais), falhas técnicas, factores externos ou fraudes, e precisa ser seguro. Um documento é seguro quando é difícil de alterá-lo. Essas características visam manter o documento autêntico, íntegro e confidencial.

---

[18] http://sis.funasa.gov.br/infcertificado/assinaturadigital.htm (18 Mai 2005)

[19] Resultado da aplicação de uma função matemática ao documento.

As assinaturas electrónicas servem para dar essas qualidades aos documentos electrónicos. As suas principais funções são a identificação da pessoa e a prova da integridade e autenticação do documento evitando alterações unilaterais.

Com a rápida expansão da Internet e o crescimento na utilização de transações por meios electrónicos (via *Internet*), a necessidade em identificar a pessoa e manter a integridade, autenticidade e confidencialidade dos documentos electrónicos tornou-se essencial para permitir o funcionamento de transações no meio digital.

A autenticidade e não-repudiação da informação são comprovados e garantidos verificando-se a chave privada do remetente, com a chave pública correspondente, já que somente o titular da chave privada poderia inseri-la em uma transação ou documento electrónico.

A integridade é comprovada e garantida com a inclusão do *hash* (resumo) da informação em conjunto com a transação ou documentos assinados digitalmente.

3.11.1 Assinatura digital de um documento

Segundo CBCE (2005), o processo de assinatura digital de um documento pode geralmente ser dividido em três etapas:

- Criação do resumo do documento;
- Assinatura digital
- Certificação digital da identidade do emissor (autenticação).
  - ✓ A primeira etapa envolve a criação do resumo do documento (*hash*), através da aplicação de uma função matemática ao documento. O resultado é um conjunto de caracteres único que representa o documento (resumo do documento). Qualquer alteração posterior ao documento implica um resumo diferente. O resumo é usado posteriormente para provar que o documento não sofreu quaisquer alterações.

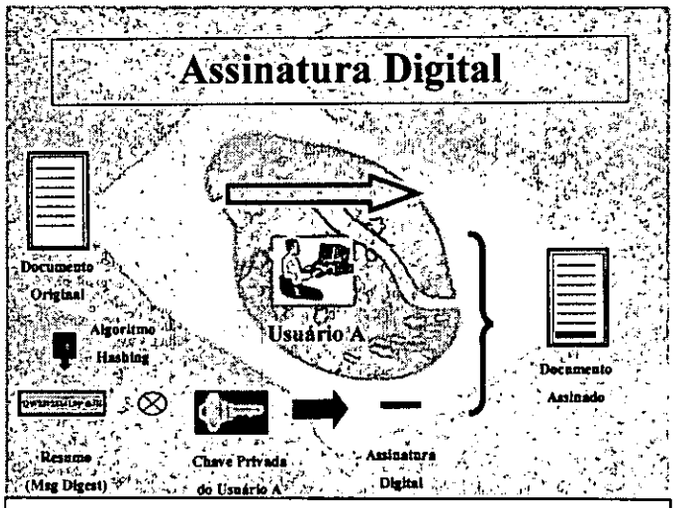


Figura 3-11: Processo de assinatura digital de um documento (CBCE, 2005).

- ✓ A segunda etapa consiste na aplicação da chave privada do emissor do documento, gerando um arquivo electrónico que representará a assinatura digital do emissor. Essa assinatura será anexada ao documento electrónico original, compondo a mensagem ou arquivo que será enviado ao receptor. Uma assinatura digital está associada a cada documento emitido.
- ✓ O terceiro passo consiste na certificação da identidade digital do emissor. Este processo envolve uma terceira entidade, a Autoridade Certificadora, que valida a identidade através do envio de uma identificação digital. Este passo garante a autenticidade da transação e prova que só o emissor (portador da chave privada usada) poderá ter a usada para assinar.

3.11.2 Verificação da assinatura digital

O receptor ao receber a mensagem ou documento original e a assinatura digital do emissor, aplica a função de *hash* ao documento original, obtendo como resultado o resumo do documento (**resumo2**).

Em seguida, a assinatura é decifrada utilizando-se a chave pública do emissor, obtendo-se o **resumo** criado pelo emissor. Compara-se o **resumo** com o **resumo2.**

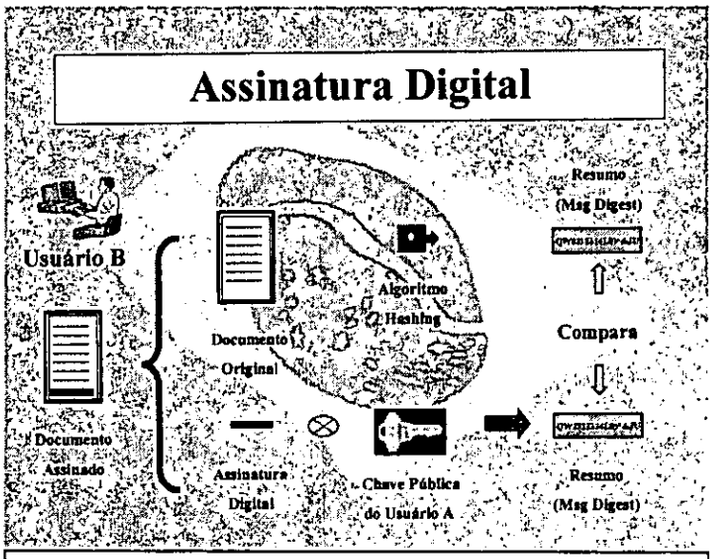


Figura 3-12: Processo de verificação da assinatura digital (CBCE, 2005).

Caso os resumos sejam iguais o destinatário poderá ter certeza que o documento não foi alterada e que o emissor é realmente o autor da mensagem.

Todas acções são executados automaticamente pelo *software* utilizado para assinar, enviar, receber e verificar assinaturas, sendo totalmente transparente para o usuário.

3.12 Legislação

As iniciativas legais com vista a disciplinar o tratamento e segurança da informação já passam a fazer parte do ordenamento jurídico dos estados e das organizações internacionais (NETO, 2003).

Para que uma Assinatura Digital seja juridicamente reconhecida, isto é, aceite como prova em tribunal, deve ter sido criada com base num certificado digital emitido por uma entidade de certificação confiável e acreditada.

4. ARQUITECTURA DA PKI PARA A REDE ELECTRÓNICA DO GOVERNO

4.1 Introdução

O presente trabalho abrange a elaboração de um modelo de PKI para a GovNet. O objectivo é criar um ambiente PKI para emitir e gerir certificados digitais que deveram ser utilizados para:

- identificar indivíduos e serviços/servidores;
- assinar digitalmente documentos e correio electrónico;
- cifrar informações.

Esta infra-estrutura oferece garantia de autenticação, integridade, confidencialidade e validade jurídica dos documentos no formato digital, assim como a autenticação de serviços/servidores de forma a permitir a realização de transacções electrónicas seguras.

A tramitação de documentos electrónicos oficiais deveria somente ocorrer quando devidamente certificada por uma entidade integrante da PKI do Governo.

4.2 Plataforma existente e sistemas instalados actualmente na GovNet

A GovNet é uma infra-estrutura de comunicação electrónica que servirá de suporte para a implementação de sistemas de informação e implantação de todas as aplicações tecnológicas de apoio às actividades de coordenação do Governo com outros sectores de utilidade pública.

Segundo UTICT (2005), presentemente, a *Intranet* da GovNet é composta por onze (11) sites conectados ao roteador central, usando cada um a largura de banda de 128kbps. Havendo em cada uma das instituições um roteador, para a conexão com a GovNet, e um *firewall*, para proteger a rede local contra acesso não autorizado.

A GovNet é uma rede com base no protocolo IP, um padrão que permite estabelecer um ambiente heterogéneo em termos de aplicações e sistemas informáticos com capacidade de suportar qualquer plataforma e aplicação que corra numa rede IP.

Presentemente a GovNet acomoda duas plataformas: plataforma *Microsoft* e a plataforma baseada em *software* de fonte aberta.

Na GovNet há cinco (5) instituições correndo a plataforma *Microsoft* (sistema operativo Windows, servidor de *e-mail exchange*, base de dados *SQL Server*, *Microsoft SharePoint Portal*, servidor de segurança ISA), as restantes instituições correm nas suas LANs a plataforma *open source* (sistema

operativo Linux, OpenOffice, servidor de e-mail, serviço de directório LDAP, e bases de dados MySQL).

As duas plataformas, interligam-se através dum VLAN *Switch* e interagem entre si providenciando serviços às onze instituições.

A nível central (na zona desmilitarizada) existem vários servidores entre os quais:

- servidor de *e-mail* – realiza a gestão de e-mail, controle de vírus e *spam*;
- servidor de aplicações - realiza a gestão de conteúdos e monitorização da rede;
- servidor de base de dados - realiza a gestão de utilizadores, publicação do website da UTICT e do Portal do Governo.

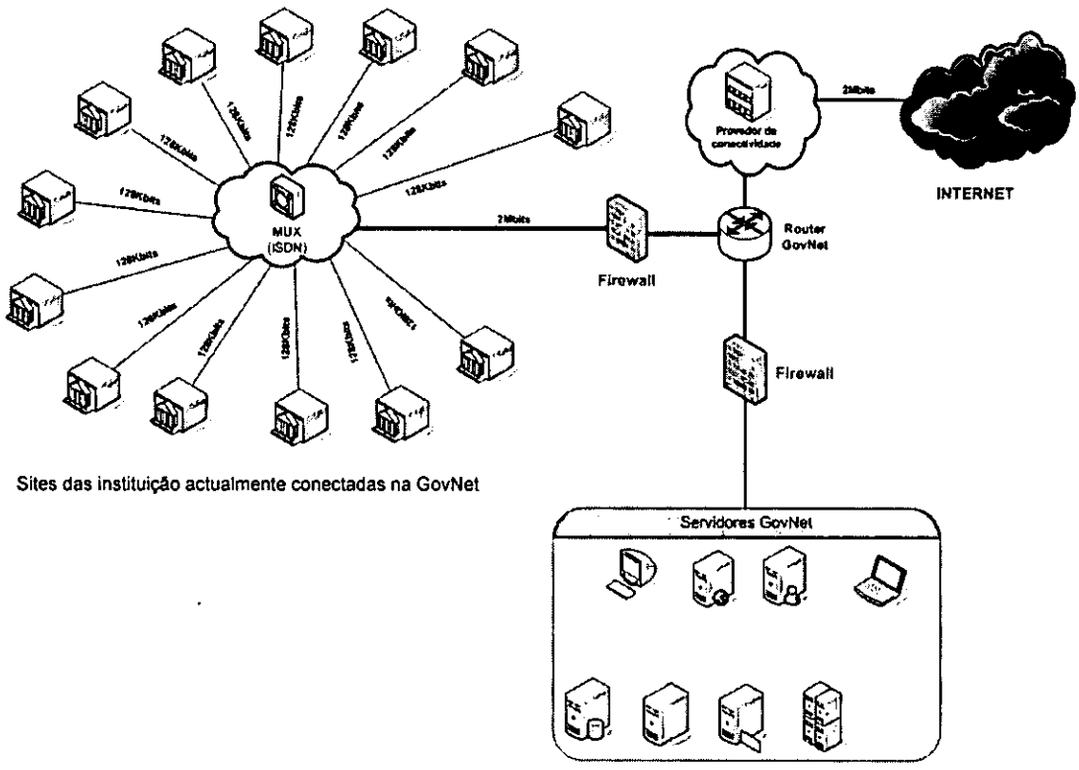


Figura 4-1: Topologia actual da GovNet (UTICT, 2005)

4.2.3 Serviços Implementados na GovNet

Segundo UTICT (2005), foram implementados três serviços básicos utilizando a rede TCP/IP: acesso à Internet, correio electrónico e mensagens instantâneas (*instant messaging*).

O sistema de *e-mail* instalado e em implementação fornece os seguintes serviços:

a) Protocolo SMTP, para o correio que entra na rede e distribuição local;

b) POP3 e/ou IMAP, para utilizadores autenticados utilizando protocolo de segurança SSL e

c) Acesso ao *webmail* para utilizadores autenticados, via Internet.

4.3 Proposta do Modelo de PKI para a GovNet

4.3.1 Padrões adoptados

Independentemente da plataforma a ser adoptada, para garantir aceitabilidade internacional e interoperabilidade da PKI em plataforma heterogénea, assim como a não vinculação a soluções proprietárias, a PKI da GovNet deve ser consistente com os seguintes padrões:

- Certificados X.509 v3
- Especificação LCRs v2 para relação de certificados revogados
- RSA PKCS#10 para solicitação de certificados
- RSA PKCS#7 para empacotamento de certificados para transporte
- RSA PKCS#1 para formato das chaves pública e privada
- RSA PKCS#12 para troca de informações pessoais
- Interface LDAP v3 para directórios X.500
- TCP/IP: Interfaces HTTP, HTTPS e SMTP para certificação de *e-mail*
- S/MIME: Certificados para clientes de *e-mail*.

A aplicação deste padrões é necessária para compatibilizar em múltiplas aplicações o formato dos certificados digitais, LCRs e assinaturas digitais, assim como a informação para o registo dos usuários.

4.3.2 Autenticação de Clientes e Servidores

O acesso a páginas web utiliza, normalmente, um sistema de autenticação não criptografado e baseado em nomes de usuários e *passwords*. Com o advento dos *Sniffers*, as *passwords* em Intranets são uma solução inadequada. Para este caso é pertinente a implementação de comunicações web seguras, aplicando o protocolo SSL e os certificados SSL para servidores, que implementa criptografia de dados, autenticação de servidores, integridade de mensagens e autenticação de usuários em conexões TCP/IP (GOLDANI, 2001*).

Na autenticação mútua de clientes e servidores, por exemplo na utilização do *webmail* da GovNet, ambos deverão fornecer os seus certificados como parte do procedimento de conexão. Se os certificados contém uma assinatura confiável (da AC que os emitiu) e as datas de validade não estão expiradas, então o cliente e o servidor são autênticos.

O processo, segundo MARTINS (2004), inicia quando o usuário conecta-se ao servidor da aplicação a aceder e ocorre a seguinte interacção:

i. O Cliente envia mensagens UDP para formação da camada de soquetes segura (SSL);

ii. O servidor verifica credenciais do usuário, formando o túnel privado virtual (VPN);

iii. O usuário acede a página web para se autenticar;

iv. O servidor requisita o certificado digital do usuário;

v. O usuário apresenta o seu certificado digital;

vi. O servidor apresenta o seu certificado digital;

vii. O servidor verifica as regras do *firewall* e autoriza o usuário a aceder a aplicação;

viii. O cliente está pronto para utilizar os recursos autorizados do servidor.

Para melhor compreensão do processo de autenticação mútua entre o usuário e o servidor usando certificados digitais para disponibiliza os serviços, a figura 4-2 apresenta sequência de forma gráfica.

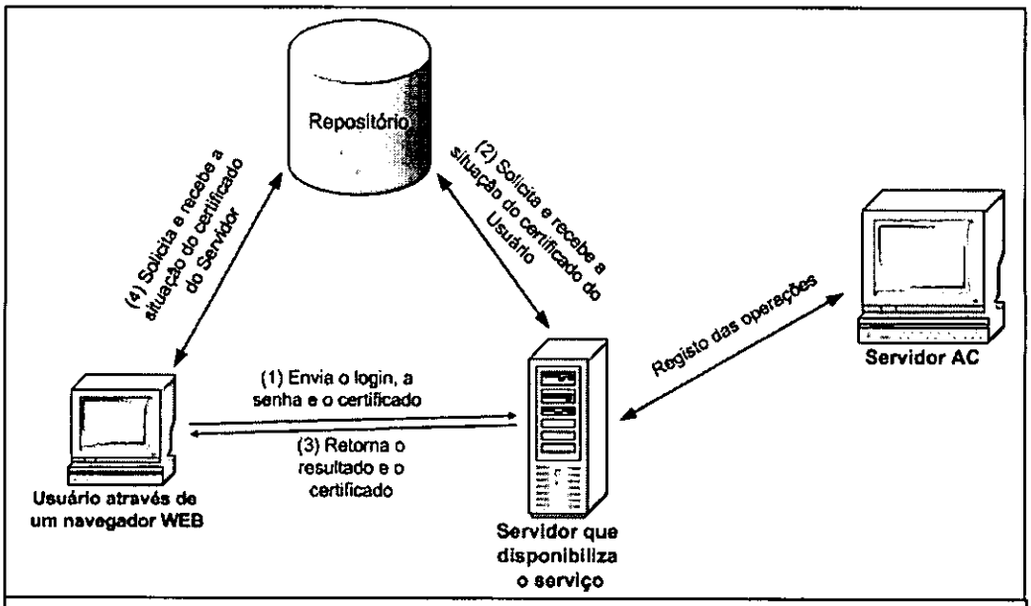


Figura 4-2: Autenticação mútua usado certificados digitais

Para a efectivação da autenticação mútua é realizada a comunicação entre o usuário, o servidor da aplicação e o repositório de certificados e LCRs para a validação de ambas partes. O Servidor da AC regista as operações de certificação realizadas. Durante a comunicações entre o cliente e o servidor os dados são criptografados e é usado o protocolo SSL.

4.3.3 Organização da PKI da GovNet

A estrutura de PKI para GovNet será composta por três níveis: o nível de gestão, o nível de credenciamento e o nível de operação.

- O nível de gestão contempla a gestão geral e a normalização da PKI.
- O nível de credenciamento contempla os métodos e processos a serem utilizados pelas instituições operacionais do sistema, com base nos regulamentos e normas preestabelecidas pelo nível de gestão.
- O nível operacional executa actividades de registo, certificação e mantém os registos das suas operações.

Figura 4-3: Organização da PKI da GovNet

A actuação das entidades em cada nível é baseada em regulamentos, normas e padrões específicos, necessários para a integração das mesmas, apresentando condições adequadas de confiabilidade técnica e operação.

4.3.4 Arquitectura da PKI da GovNet

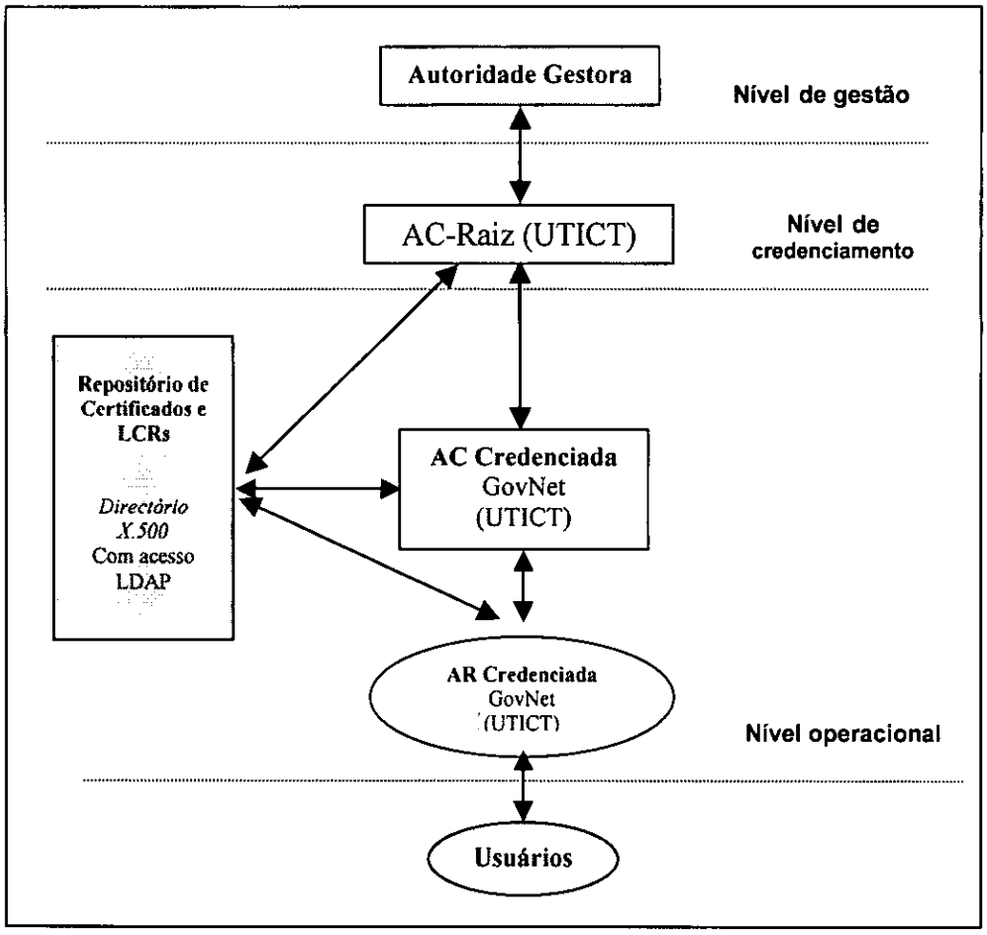


Figura 4-4: Componentes básicos da PKI da GovNet

4.3.4.1 Autoridade Gestora

Compete à Autoridade Gestora (AG):

- Propor a criação da AC-Raiz, estabelecer, avaliar e aprovar políticas, critérios e normas no âmbito da PKI da GovNet, seja para as ACs e ARs ou supervisão da AC-Raiz;
- Propor e implementar acordos internacionais com PKIs externas relativos a certificação cruzada, regras de interoperabilidade, entre outros.

Para o credenciamento das entidades integrantes da PKI da GovNet a AG deve aprovar critérios e procedimentos para o credenciamento, manutenção e descredenciamento das ACs e ARs, atendendo um conjunto de requisitos no que refere a personalidade jurídica e requisitos técnicos determinados.

4.3.4.2 Autoridade Certificadora Raiz

A AC-Raiz da cadeia de certificação da GovNet é responsável pelo credenciamento na cadeia hierárquica, operando a partir das definições da Autoridade Gestora.

No modelo proposto neste trabalho, AC-Raiz irá operar apenas no âmbito da GovNet, credenciando apenas uma AC e uma AR. Contudo, esta arquitectura é escalável e futuramente poderão ser admitidas outras ACs e as respectivas ARs, quer privadas ou públicas para permitir o uso generalizado dos certificados digitais, possibilitando deste modo o desenvolvimento do comércio electrónico em Moçambique.

Compete a AC-Raiz:

- emitir, distribuir, revogar, renovar e gerir os certificados das ACs subordinadas, quer públicas ou privadas, bem como gerir a Lista de Certificados Revogados;
- auditar e fiscalizar as ACs e ARs, prestadoras de serviços credenciados na infra-estrutura.

Este modelo foi concebido tendo como base a estrutura da GovNet já existe implementada pela UTICT. Por esta razão e por questões funcionais deverão ser criados os níveis necessários na UTICT de modo a suportar a estrutura de PKI (AC-Raiz, AC e AR) na fase inicial (projecto piloto).

4.3.4.3 Autoridade Certificadora

A AC é a responsável por todo o ciclo de certificação e é a primeira entidade do nível operacional do sistema, credenciada pela AC-Raiz.

São competências da AC:

- emitir, distribuir, revogar, renovar e gerir os certificados para os usuários finais, bem como gerir a Lista de Certificados Revogados dos mesmos;
- manter registos de suas operações.

As ACs deve apresentar seguro de responsabilidade civil para os serviços de certificação digital e ter suas instalações em território nacional.

A AC tem obrigação de transparência em suas actividades, seja para garantir segurança na medida que o usuário tem conhecimento dos certificados revogados e pode consultar as operações já realizadas.

4.3.4.3.1 *Hardware Security Module*

Hardware Security Module (HSM) é uma componente obrigatória em um ambiente PKI para assinaturas digitais. Usando o HSM, todo o armazenamento de chaves e operações de criptografia da AC são realizadas dentro de um hardware seguro, onde não são acessíveis pelo mundo externo.[20]

Todos acessos ao HSM estão sujeitas a controle e podem ser armazenados em arquivo de log.

Performance

- O HSM acelera os serviços de criptografia da AC com o seu processador criptográfico *on-board* (operações simétricas e assimétricas).
- Diminui o tempo consumido pelo processador do Servidor da AC com operações criptográficas, a CPU do Servidor é liberada para realizar operações mais críticas.

4.3.4.4 Autoridade de Registo

A AR é fundamental para descentralizar o serviço da AC, age como a interface da PKI com o usuário final, ela é vinculada à AC tendo as seguintes competências:

- identificar e registar usuários presencialmente;
- enviar a AC o requerimento impresso e também no formato electrónico subscrito pelo requerente, solicitando a emissão do certificado;
- manter os registos de suas operações.

4.3.4.5 Usuários

Compete aos usuários da GovNet:

- a sua inscrição e identificação adequada, durante o processo da requisição do certificado;
- utilizar os certificados para fins estritamente indicados na política de certificados.
- solicitar a revogação do certificado, quando haver suspeitas da apropriação da chave privada por terceiro.
- observar todos os procedimentos de segurança e protecção de suas chaves privadas.
- O usuário deve ter a habilidade de analisar a estrutura (pessoa ou entidade, emitente, assinatura digital do emitente, número serial e período de validade).

[20] **ERACOM TECHNOLOGIES**. http://www.eracom-tech.com (18 Jul 2005)

4.3.4.6 Repositório de certificados e Lista de Certificados Revogados

O sistema de armazenamento proposto é o directório X.500 com acesso LDAP também conhecido por X.500-Light que pode ser usado na Internet. Foi seleccionado tendo em consideração a escalabilidade e compatibilidade com as aplicações existentes actualmente na GovNet, para além de que o LDAP já está sendo usado em algumas instituições integrantes da GovNet.

As LCRs serão publicadas na página de Internet, onde também serão disponibilizados os certificados da AC-Raiz e AC da GovNet, assim como dos usuários.

4.4 Política de Segurança

Segundo UTICT, (2005*), a política de segurança da GovNet estabelece as directrizes de segurança para todos os integrantes da rede. As regras gerais da política de segurança estabelecem o princípio de gestão da segurança abrangendo os recursos humanos e tecnológicos das instituições que integram a GovNet, determinando ainda a ampla divulgação dos procedimentos previstos para garantir a segurança.

A política de segurança da GovNet, não preconiza a utilização da certificação digital e das assinaturas digitais, contudo a introdução da PKI tem o seu enquadramento no que concerne a política do uso de correio electrónico na GovNet, política de encriptação a aceitável e política da Rede Privada Virtual (VPN).

De acordo com a apresentação realizada na secção 3.8.2, os três (3) elementos apresentados acima baseiam-se em aplicações que foram projectadas para operar com a PKI.

É de notar que a política de segurança da GovNet ainda não foi aprovada e está a ser melhorada, no entanto, na sua versão final poderá incluir os aspectos pertinentes a utilização da certificação digital e assinaturas digitais.

4.5 Declaração de Práticas de Certificação da AC-Raiz

Este documento descreve as práticas e procedimentos aplicados pela AC-Raiz na PKI da GovNet no exercício das suas funções.

A AC-Raiz possui o certificado de nível mais alto, este certificado contém a chave pública correspondente à chave privada da própria AC-Raiz utilizada para assinar seu próprio certificado e os certificados das ACs do nível imediatamente subsequente ao seu e a sua Lista de Certificados Revogados.

4.6 Política de Certificados da AC - PKI da GovNet

A Política de Certificados define duas classes de certificados no âmbito da PKI da GovNet, que atendam às necessidades gerais da maioria das aplicações na administração pública.

Serão imitidos os seguintes tipos de certificados:

1. **Certificados de assinatura digital** - usados para assinar digitalmente, vinculando uma chave pública ao seu titular e para cifrar as informações, tendo a seguinte aplicabilidade:
   - assinatura e encriptação de mensagens de correio electrónico;
   - assinatura digital e encriptação de documentos electrónicos;
   - transações *online*, e em redes privadas virtuais;
   - troca de chaves para a encriptação de dados; e
   - autenticação para acesso a sistemas electrónicos.

   O certificado de assinatura digital é gerado e armazenado no USB Token que pode ser conectado a qualquer computador através da porta USB. Tem a validade de 2 (dois) anos.

   Os certificados de assinatura digital podem ser emitidos para pessoas físicas e para organizações pública ou privadas.

   Para requerer um certificado digital o requerente deve fornecer os seguintes dados, que constarão na identidade digital:

   1. Nome
   2. NUIT
   3. Morada/Endereço*
   4. Telefone
   5. E-mail
   6. Data de nascimento/Ano de fundação*
   7. Chave pública
   8. Termo de adesão assinado

   * *No caso de ser uma organização*

2. **Certificados Digitais SSL (Servidor seguro)**

   Os certificados digitais SSL, com selo de segurança, oferecem uma plataforma de autenticação de serviços/sites e confiança para a realização de transações *online* seguras.

   Os certificados digitais SSL serão emitidos para websites ou servidores.

Para requerer um certificado Digital SSL para além do Contrato assinado o requerente deverá fornecer os seguintes dados, que constarão na identidade digital do servidor ou website:

1. Nome do website/servidor
2. Tipo de Serviço
3. Proprietário
4. Endereço do proprietário
5. Telefone do proprietário
6. E-mail do proprietário
7. Chave pública

4.7 Declarações de Práticas de Certificação da AC - PKI da GovNet

Este documento descreve as normas e procedimentos aplicáveis na AC da GovNet para a implementação da política de certificação proposta.

A PKI da GovNet suportará três níveis de certificados. O primeiro nível contém um único certificado da AC-Raiz, de titularidade da UTICT. No segundo nível, estarão os certificados das ACs. O terceiro nível corresponde aos certificados de usuários finais.

Revogação do certificado

A revogação do certificado será feita:

- a pedido do usuário, em caso de perda do controle da chave privada ou haver dúvidas sobre a sua segurança;
- quando o usuário for excluído da GovNet;
- se a AC detectar alguma irregularidade no uso certificado.

A Lista de Certificados Revogados será actualizada mensalmente.

Os certificados expirados serão mantidos arquivados por trinta anos.

Os dados e informações das entidades serão protegidos contra ameaças e acções não autorizadas. As violações de segurança serão registadas e analisadas periodicamente.

Armazenamento das Chaves Privadas

Existem vários suportes para o armazenamento das chaves privadas e dos certificados digitais pessoais, como foi discutido na secção 3.9.4.

Na PKI da GovNet será adoptado o *USB Token* para o armazenamento da chave privada e certificado pessoal.

Quando for preciso realizar operações que envolvem objectos privados, o módulo de segurança recupera a chave privada necessária no token após satisfazer os requisitos de autenticação com um PIN (número de identificação pessoal) de usuário que se for introduzido incorrectamente três vezes bloqueia o token.

Este sistema de segurança baseia-se na chave privada para garantir a confidencialidade, integridade e não repudiciação da informação. Contudo, no caso do titular perder a sua chave privada não haveria hipótese nenhuma de recuperar todos os documentos cifrados com a sua respectiva chave pública.

Por este motivo a AC utilizando mecanismos apropriados deve guardar uma cópia da chave. Este procedimento pode levantar suspeitas e o titular da chave poderia alegar que alguém com acesso à AC teria usado a sua chave, fazendo-se passar por ele para assinar determinada mensagem, quebrando desta forma princípio de não repudiciação da informação.

Para eliminar este dilema, deve-se adoptar o modelo "*Dual-Key Pair*", isto é cada utilizador terá dois pares de chaves, um para assinar e outro para cifrar. A chave privada de assinatura encontra-se na posse do seu titular guardada no *token* e a de cifra tanto se encontra na posse do titular, como é guardada uma cópia daquela nas bases de dados da AC.

Segundo CARVALHO (2003), adoptando este modelo, pode-se garantir com toda certeza que apenas quem esteve na posse do *token* e conhecia o PIN, poderia ter assinado determinado documento.

O titular deve manter o PIN secreto e em caso de extravio do token, deve imediatamente solicitar a revogação do certificado.

PROCEDIMENTOS DE SEGURANÇA

Protecção da chave privada da AC

A chave privada da AC deverá ser guarda no Módulo de Segurança em Hardware que oferece várias características de segurança discutidas na secção 3.9.4.

A chave privada em uso deverá estar criptografada usando a criptografia simétrica de, no mínimo, 128 bits, e contar com medidas físicas de contenção do acesso por terceiros. O uso da chave privada, para assinatura dos certificados das ACs e das Listas de Revogação de Certificados, dependerá da presença de 2 (duas) pessoas, no mínimo.

Cópias de segurança

A AC-Raiz e as ACs deverão manter cópias de segurança actualizadas dos certificados expedidos e de todos os dados a eles relativos. Deverão manter também as cópias de segurança de suas próprias chaves privadas, para o caso de destruição da chave em uso. A cópia de segurança deverá estar criptografada.

4.8 Processo de emissão do certificado

O processo inicia quando um usuário gera localmente um par de chaves pública/privada utilizando a interface web disponibilizada pela AR e gera uma requisição com a sintaxe definida pelo PKCS#10 que é enviada a AR solicitando a emissão do certificado. O pedido de emissão pode ser realizado via Internet ou por meio do *e-mail*. O usuário deverá também submeter um requerimento impresso e se apresentar na AR para efeitos de identificação pessoal, apresentado o seu documento de identidade.

A AR analisa esta solicitação segundo a sua política definida e, se concorda, envia o pedido de emissão à AC, esta verifica por sua vez os dados se concordar emite o certificado, grava-o, gera o par de chaves no token e publica-o no repositório de certificados.

Procede-se então o envio do lote à AR, esta fará a impressão dos PINs correspondestes aos pedidos e procederá a publicação dos certificados via LDAP. A resposta ao requerente do certificado é enviada no formato PKCS#7 (envelope assinado).

O PIN será entregue pessoalmente ao titular do certificado para garantir segurança e confidencialidade. De referir que o único PIN que a AR retém é o inicial, o qual o utilizador deverá alterá-lo de imediato.

Todo o tráfego é mantido privado entre o usuário e a AR. O processo de pedido de revogação de um certificado é idêntico ao pedido de emissão de certificado, à excepção de, em lugar de emitir certificado solicita-se a revogação. Os pedidos são realizados via web ou por *e-mail*.

A figura 4-4, na página seguinte, ilustra o processo de emissão de um certificado digital, mostrando as acções do requente ao desencadear o processo de pedido de emissão do certifica; seguindo-se a validação ou rejeição do pedido pela AR e por a emissão e publicação do certificado pela AC.

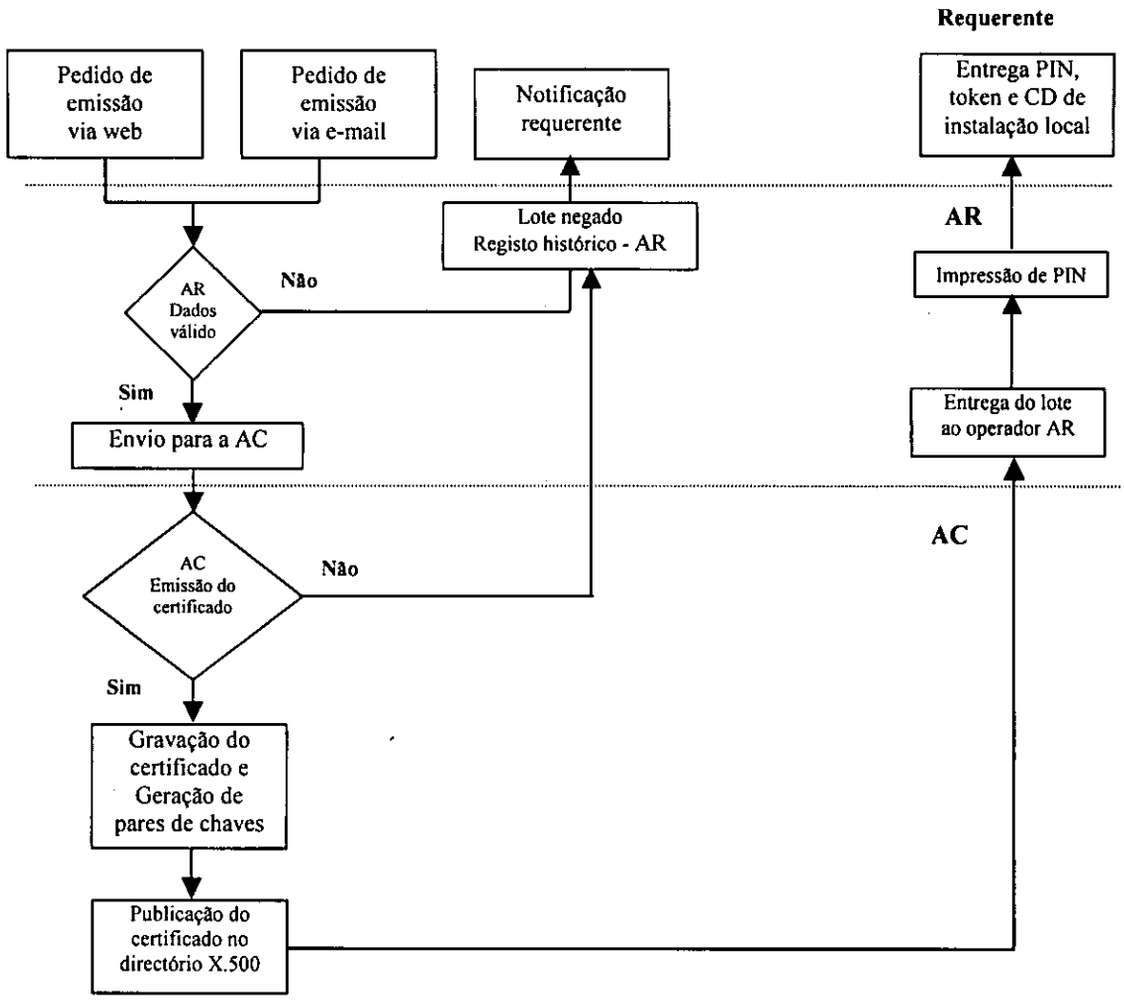


Figura 4-5: Ciclo de emissão de um certificado digital

4.9 Publicação dos Certificados Digitais

Os certificados serão publicados no directório público X.500, podendo um usuário armazenar no seu computador os certificados que chegarem juntamente com as mensagens assinadas. O receptor ficará na posse da chave pública daquele emissor, podendo fazer uso dela quando pretender enviar-lhe mensagens cifradas ou cifrar documentos.

Doutro lado, para utilização interna, na *intranet* da GovNet, em aplicações como bases de dados que requerem a utilização de certificados automaticamente. Os certificados e respectivas chaves públicas serão publicadas no servidor de directório[21] de utilizadores do sub-domínio[22] onde estão

[21] O servidor de directório contém as contas dos utilizadores, permite a autenticação e controle dos privilégios dos utilizadores na rede.

localizadas as respectivas contas dos seus titulares, havendo depois uma replicação para os servidores de directório dos restantes sub-domínios da GovNet. Deste modo todas aplicações terão acesso à mesma informação.

A publicação de chaves públicas e respectivos certificados na *Intranet* da GovNet, assim como a comunicação entre os servidores de directório dos sub-domínios será efectuada via LDAP, bastando pesquisar no directório o utilizador em questão e gravar no atributo correcto o seu certificado digital com a correspondente chave pública.

Esta operação é realizada de um modo transparente através de pequenos *scripts*.

É de notar que uma eventual actualização/renovação ao certificado, será aplicada automaticamente no directório, situação que não acontecerá com os certificados guardados no computador pessoal.

4.10 Lista de Certificados Revogados

A Lista de Certificados Revogados é uma lista de certificado cancelados. Os certificados expirados não são incluídos nesta relação. A lista contém os números seriais dos certificados associados com um indicador do motivo da revogação. Este valores serão datados e assinados pela CA.

4.11 Interacção das entidades da PKI da GovNet

A **interface web** é o canal usado para a interacção do usuário com o sistema. Através dela o usuário pode obter os certificados das autoridades existentes, solicitar e acompanhar o estágio do processo de emissão do seu certificado.

Os **servidores** da AC-Raiz, AC, AR e Web executam toda a interacção com o repositório de certificados.

- O servidor da AC-Raiz interagem com o repositório para a publicação do seu próprio certificado e dos certificados das ACs a ela subordinadas e a respectiva LCRs.
- O **operador da AR** entre outras funções, aprova as requisições feitas pelos usuários via interface web, e os dados são depositados no repositório para serem acedidos pela AC e pelo próprio usuário.
- O **operador da AC** obtém as solicitações de certificados aprovadas pela AR e decide sobre a emissão ou não dos certificados. O resultado das acções são novamente armazenadas no repositório para efeito de informação ao usuário final.

[22] Os sub-domínios da GovNet são os domínio existentes em cada instituição integrante, onde são criadas as contas dos utilizadores dessa instituição.

O **Servidor Web** juntamente com **Servidor da AR** respondem as acções enviadas pelos usuários. A figura 4.5 mostra as interacções descritas acima que ocorrem na PKI.

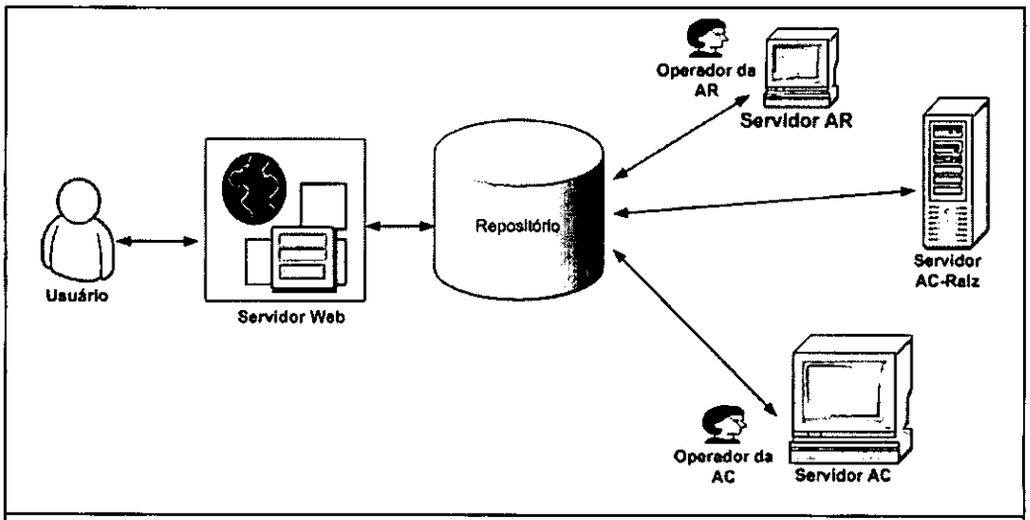


Figura 4-6: Interacção das entidades na PKI da GovNet

4.12 Integração da PKI na infra-estrutura existente da GovNet

O servidor da AC-Raiz tem a função de emitir e gerir os certificados das ACs a ela subordinadas e revogação das suas chaves públicas emitindo a respectiva LCRs. O modelo proposto possui uma única AC, mas futuramente pode ser necessário descentralizar o serviço de emissão de certificados, distribuindo geograficamente por pontos estratégicos do país as ACs com as respectivas ARs a si conectadas.

O servidor da AC é o responsável por todo o ciclo de certificação dos usuários finais. Tem a função de emitir, gerir, revogar, publicar os certificados digitais e as LCRs no repositório e registar as operações realizadas com a certificação digital da PKI da GovNet. Também tem a função de armazenar os registos das suas operações e recuperar as chaves criptográficas. Esta função é necessária para o acesso de arquivos criptografados caso a chave privada seja perdida ou danificada.

O servidor da AR tem a função de processar os dados para o registo dos usuários, descentralizando deste modo o serviço da AC e assume a parte administrativa da actividade para além de armazenar os registos das suas operações.

O repositório de certificados e LCRs tem a função de armazenar e disponibilizar os certificados e LCRs aos usuários da PKI a qualquer momento.

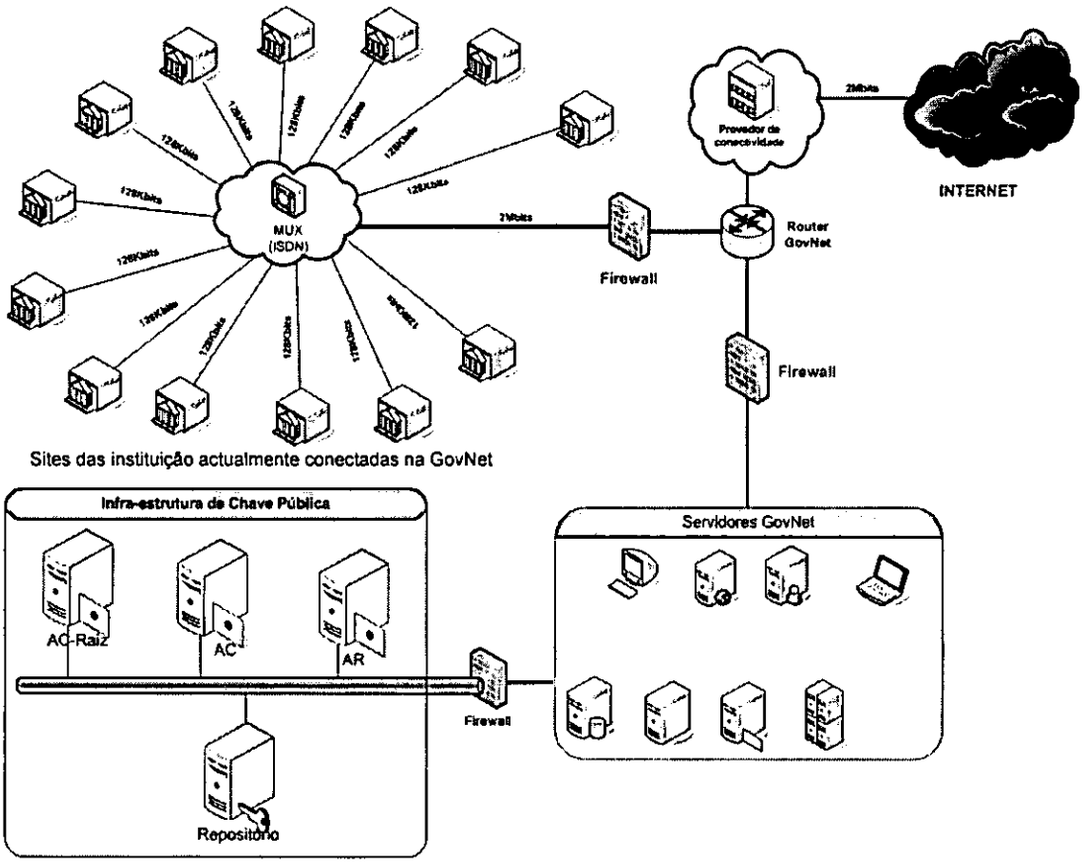


Figura 4-7: Topologia da GovNet com a Integração da PKI

Os servidores da AC-Raiz, AC, AR e Repositório de certificados serão localizados na rede interna da UTICT protegidos por uma *firewall* interna para aumentar a sua protecção contra ataques externos. A figura 4-7 ilustra a rede da GovNet com a integração da PKI proposta.

O servidor web para a publicação e requisição de certificados ou pedido de revogação será localizado, por questões de segurança, na Zona Desmilitarizada (DMZ) da rede da UTICT, onde será instalada a interface web para a interacção com o usuário. Para este fim pode ser usado o servidor Web da UTICT usado actualmente para publicar páginas web e o portal do Governo.

A integração da PKI no sistema já existe da GovNet, para além de eliminar o problema relacionado com a distribuição de chaves e garantir a vinculação da chave pública dos usuários e servidores, evitando deste modo a falsificação da identidade electrónica, irá adicionar as seguintes funcionalidades:

- comunicações seguras: onde os usuários poderão estabelecer comunicações, sendo possível verificar a integridade dos documentos com a assinatura digital dos documentos e correio electrónico e toda a informação que circula pelo meio de transmissão de dados será criptografada;

- verificação e autenticação de serviços/sites de Internet com a utilização dos certificados para servidores, assim como a autenticação mútua entre o usuário e servidor.
- A Autoridade Certificadora funcionará como um "cartório electrónico", permitindo deste modo a validade jurídica dos documentos assinados electronicamente, dando-os o mesmo valor como os documentos em papel assinados pelo punho da mão. Desta forma os documentos electrónicos adquirem o valor probatório e quem envia um documento com a sua assinatura electrónica não terá como negar a sua autoria.

Em suma, a implementação da PKI da GovNet irá prover a rede de meios para preservar a segurança da informação em transações electrónicas, garantindo as premissas de Confidencialidade, Integridade, Identidade (não-repúdio) e autenticidade.

4.13 Utilização dos certificados digitais na GovNet

Os certificados serão utilizados maioritariamente na validação de informação assinada digitalmente, esse processo consiste geralmente nos seguintes passos:

1. O destinatário verifica que a identidade indicada pelo emissor está de acordo com a identidade indicada no certificado;
2. O destinatário verifica que o certificado é válido:

   . que a assinatura do certificado é válida;

   . que foi efectuada por uma autoridade de certificação de confiança;

   . que o certificado está dentro do seu período de validade;
3. O destinatário utiliza a chave pública contida no certificado para verificar a assinatura digital da informação recebida (vide 3.11.2).

Se todos os passos anteriores forem executados sem problemas, o destinatário aceita que a informação foi assinada pelo emissor, e que essa informação permanece inalterada.

Outra aplicação importante dos certificados digitais é a autenticação dos serviços ou sites para a realização de transações seguras , principalmente no comércio electrónico.

Para que o certificado da AC da GovNet seja reconhecido pelos *browers* é necessários que seja instalado nos mesmos. Algumas ACs solicitam aos fabricantes dos *browsers* a pré-instalação dos seus certificados para que sejam reconhecidos automaticamente.

Uma AC que não tenha os seus certificados pré-instalados nos *browsers*, pode solicitar a assinatura do seu certificado a uma AC com o certificado pré-instalado no *browser*, passando a fazer parte da hierarquia dessa AC, deste modo o seu certificado será reconhecido.

Outra alternativa é a disponibilização ao público do seu certificado para que os usuários possam fazer o *download* e instalação nos seus *browsers*.

A AC da GovNet não será colocada a nenhuma hierarquia de ACs já existentes, cujos os certificados são reconhecidas pelos *browsers*. No entanto, serão disponibilizados pela Internet o certificado da AC-Raiz da GovNet para que os usuários façam, uma única vez, o *download* e instalação (vide Anexo 3), passando deste modo a ser reconhecida pelo *browser* como uma AC confiável.

5. CONCLUSÃO

A troca da informação confidencial na GovNet, assim como as transações bancárias, comércio electrónico, entre outros serviços, precisam de uma segurança específica e uma garantia de ambos participantes na transacção.

Apenas um mecanismo de segurança não é suficiente para garantir a segurança de uma rede ou sistema, é necessário o desdobramento de vários mecanismos. Uma política de segurança é uma boa base de informação ao usuário e aos administradores de redes/sistemas e torna-se fundamental a utilização dos certificados digitais.

A introdução da certificação digital na GovNet garantirá os princípios básicos da comunicação segura em ambiente de rede de computadores como: autenticação de usuários e serviços/sites de forma efectiva usando certificados digitais (autenticação mútua), confidencialidade e integridade dos documentos electrónicos, para além da gestão de chaves criptográficas e não-repudiação da informação emitida.

O facto de não haver possibilidade de falsificar uma assinatura electrónica, porque é única e diferente para cada documento, garante que a pessoa que assinou um documento é realmente quem diz ser e é possível verificar se um documento foi alterado. Estes aspectos reduzirão a desconfiança e insegurança na GovNet.

No nosso país não há legislação específica em diversas áreas de Tecnologias de Informação e Comunicação, o que não permite, neste caso concreto, o reconhecimento legal dos documentos e transações electrónicas.

A utilização dos certificados e assinaturas digitais emitidos e administrados pela AC da GovNet que será uma entidade idónea e que funcionará como um "cartório electrónico", garantindo a autenticação dos documentos electrónicos, validação das partes nas transações e registo das operações, se for acompanhada com a criação da legislação inerente garantirá o reconhecimento jurídico dos documentos e mensagens em meios electrónicos.

A implementação da PKI na GovNet, permitirá a redução da burocracia e do espaço físico para a guarda dos documentos, para além do aumento da eficiência, agilidade nos processos e também proporcionará uma oportunidade para a geração de emprego e negócio, pois permitirá o surgimento de empresas dedicadas aos serviços de certificação digital para o público em geral.

6. RECOMENDAÇÕES

Para além do modelo proposto, a PKI da GovNet deverá contemplar um conjunto de regulamentos e normas de funcionamento aprovadas por lei para o enquadramento legal das suas operações.

Para garantir o reconhecimento jurídico da PKI da GovNet e sobretudo dos documentos no formato electrónico, a PKI da GovNet deve ser instituída nos termos da lei e também deve ser estabelecido nos mesmos as competências de cada entidade integrante na estrutura.

É necessária a criação da legislação específica em Moçambique que permita o reconhecimento jurídico dos documentos e transações electrónicas com base na utilização dos certificados digitais.

A Autoridade Gestora deve ser o primeiro órgão a ser criado e este por sua vez irá instituir a PKI e os órgão a ela subordinados.

Recomenda-se a inclusão na política de segurança da GovNet dos aspectos referentes a utilização da certificação digital e assinaturas digitais.

Para garantir o sucesso da PKI, devem ser realizados programas contínuos de capacitação e informação dos usuários da GovNet sobre a importância, funcionamento e uso da PKI, assim como para a divulgação da política de segurança da GovNet.

A solução de software recomendada para a implementação da PKI da GovNet é o NewPKI (vide anexos).

7. BIBLIOGRAFIA

(BARBOSA, 2005) **BARBOSA**, M. (2005) *Certificação e Public Key Infrastruture (PKI).* http://wiki.di.uminho.pt/wiki/pub/Education/CriptografiaAplicada/CA-Mod2.pdf (18 Abr 2005)

(CANDÉA, 2002) **CANDÉA,** S. (2002) *Colectânea de recomendações básicas de segurança de sistemas, destinadas aos administradores de rede.* Instituto Tecnológico de Aeronáutica , São José dos Campos, BR

(CBCE, 2005) **CBCE. Câmara Brasileira de Comércio Electrónico** (2005). *Certificação digital.* CBCE. (s.l.) BR

http://www.ibpbrasil.com.br/certificacaodigital/images/guia.pdf

(29 Jun 2005)

(CARVALHO, 2003) **CARVALHO,** C. (2003) *Infra-estrutura de Chave Pública do Ministério da Justiça.* Universidade de Lisboa. Lisboa, PT

(GOLDANI, 2000) **GOLDANI,** C. (2000) *Sistemas de certificação digital X.509 e PKIX.* UniCERT Brasil, (s.l.). http://www.unicert.com.br/files/pdf/certificacao.PDF (07 Abr 2005)

(GOLDANI, 2001) **GOLDANI,** C. (2001) *Padrões Relacionados com o PKI.* UniCERT Brasil, (s.l.). http://www.unicert.com.br/files/doc/unicert11.doc (07 Abr 2005)

(GOLDANI, 2001*) **GOLDANI,** C. (2001*) *Infraestrutura de Chave Pública em Redes Corporativas.* UniCERT Brasil, (s.l.). http://www.unicert.com.br/files/doc/unicert10.doc (11 Abr 2005)

(ITI, 2005) **ITI**. Instituto Nacional de Tecnologia de Informação – Brasil (2005) *Vídeo sobre certificação digital e software de código livre.* http://www.iti.gov.br (04 Fev. 2005)

(LEMOS, 2001) **LEMOS,** A. (2001) *Política de segurança da informação.* Universidade Estácio de Sá. Rio de Janeiro. BR. http://www.estacio.br/campus/millorfernandes/monografias/aline_morais.pdf (20 Mai 2005)

(MACHADO, 2002) **MACHADO,** M. (2002) *Análise e estudo de segurança de corporações utilizando firewalls.* Universidade Federal do Espírito Santo. Victória, BR

(MAIA, 2005) **MAIA,** M. (2005) *Gestão de Riscos: o que avaliar?*

Módulo Security Magazine: http://www.modulo.com.br/index.jsp?page=3&catid=2&objid=431&pagecounter=0&idiom=0 (22 Mar 2005)

(MARTINS, 2004) **MARTINS,** A. (2004) *Estudo e implantação de infra-estrutura de chave pública com aplicação em controle de acesso sem fio.* Universidade Federal do Rio de Janeiro. Rio de Janeiro. BR

(NETO, 2003) **NETO**, C. (2003). *Segurança da informação corporativa: Aspectos e implicações jurídicas*. Centro de Ciências Jurídicas. Campina Grande, BR

(PAULINO, 2003) **PAULINO,** N. (2003) O *que é o ssh?*

In: News Generations: Boletim bimestral sobre tecnologia de redes. Vol 1, N°3 (Agosto 2003). Rede Nacional de Ensino e Pesquisa. (s.l.). BR. *http://www.rnp.br/newsgen/9708/n3-3.html* (28 Jun 2005)

(PINHO, ?) **PINHO, M. (?)** *Certificação digital no combate à burocracia*

http://www.certisign.com.br/certinews/cpalavra/material_03.jsp (20 Jan. 2005)

(SELEGUIM, 2003) **SELEGUIM**, G. (2003) *Segurança da Informação: Perigos do Mundo Virtual.* Pontifícia Universidade Católica de Campinas, BR

(SILVA, 2004) **SILVA,** B. (2004) *Uma abordagem de infra-estrutura de chaves públicas para ambientes corporativos*. UNICEUB. Brasília, BR

(STANTON, 2002) **STANTON,** M. (2002*). Processamento dinâmico de caminhos de certificação em ambientes distribuidos de grande porte.* In: NewsGeneration. Boletim bimestral sobre tecnologia de rede. Vol. 6, No. 2 (12 de Abril de 2002).

http://www.rnp.br/newsgen/0203/processamento_dinamico.html#ng-2-1 (04 Mai 2005)

(SYMANTEC, 2004) **SYMANTEC** (2004) *ISO 17799: o padrão de segurança global emergente. http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=395&pagenumber=0&idiom=0 (22 Mar 2005*

(UTICT, 2005) **UTICT. Unidade Técnica de Implementação da Política de Informática** (2005) *Projecto de Rede Electrónica do Governo (fase piloto): Relatório final do projecto*. UTICT, Maputo, MZ

(UTICT, 2005*) **UTICT. Unidade Técnica de Implementação da Política de Informática** (2005) *Política de segurança*. UTICT, Maputo, MZ

(VELOSO, 2002) **VELOSO**, C. (2002) *Criptologia: Uma ciência fundamental para tratamento de informações sigilosas*. Escola do Governo de Minas Gerais, Minas Gerais, BR

(XENITELLIS, 2000) **XENITELLIS**, S. (2000) *The Open-source PKI Book: A guide to PKIs and Open-source Implementations*. http://ospkibook.sourceforge.net/ (29 Mar 2005)

(XEXÉO, ?) **XEXÉO, G.** (?) *Autenticação de documentos digitais por sistemas criptográficos de chave pública*. http://www.projectoderedes.kit.net (28 Mar 2005)

BIBLIOGRAFIA NÃO REFERENCIADA

(CERTISIGN, 2005) **BRASIL. CERTISIGN**, (2005) *Primeira leitura sobre certificação digital* http://www.certisign.com.br/ (09 de Jan. 2005)

(KUHN, 2001) **KUHN,** D. (2001) *Introduction to Public Key Technology and the Federal PKI Infrastructure*. National Institute of Standards and Technology, (s.l.) http://www.modulo.com.br/pdf/de010226-pki.pdf (07 Fev. 2005)

(MACOME, 1995) **MACOME**, E. (1995) *Introdução à metodologia de investigação*. UEM, Maputo, MZ

(MICROSOFT, 2004) **MICROSOFT** (2004) *About Certificate Enrollment Control. Platform SDK.* http://www.msdn.microsoft.com/library/default.asp?url=/library/en-us/security/xen_abus_66cs.asp (09 Dez. 2004)

(MICROSOFT, 2004) **MICROSOFT** (2004) *Projetando sua Infra-estrutura de Chave Pública.* http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod170.mspx (09 Jan. 2005)

(SARAIVA, 2003) **SARAIVA,** E (2003) *Entendendo a infraestrutura de chave pública.* http://sisnema.com.br/forums/ShowPost.aspx?PostID=10892 (09 Jan. 2005)

(SOUZA, .2005) **SOUZA**, L. (2005) *Como garantir a segurança física de redes de computadores e CPDs*. Universidade Estácio de Sá. Rio de Janeiro, BR http://www.modulo.com.br/index.jsp?page=3&catid=17&objid=63&pagecounter=0&idiom=0 (01 Abr 2005)

(TORRES, ?) **TORRES,** M. (?) *Tecnologias da Infra-estrutura de Informação em Ambientes Colaborativos de Ensino: Comércio Eletrônico - Estudo de Caso*. Universidade Estadual de Campinas – Unicampo, BR http://www.dca.fee.unicamp.br/courses/IA368F/1s1998/Monografias/flavia/e-commerce.html#3.3.%20Esquema%20de%20Segurança (28 Mar 2005)

ANEXOS

Anexo 1: GLOSSÁRIO

Acesso remoto – Comunicação entre computadores ou outro dispositivo de conexão que estão distantes, é feita normalmente através da Internet;

***Application Programming Interface* (API)** - é um conjunto de rotinas e padrões estabelecidos por um *software* para utilização de suas funcionalidades. De modo geral, a API é composta por uma série de funções acessíveis somente por programação. Por exemplo, um sistema operacional (como o Windows) possui uma grande quantidade de funções na API, que permitem ao programador criar janelas, aceder arquivos, criptografar dados, etc;

Assinatura Digital - É um conjunto de procedimentos matemáticos realizados com a utilização de técnicas de criptografia, o que permite, de forma única e exclusiva, a comprovação da autoria de um determinado conjunto de dados de computador (um arquivo, um e-mail ou uma transação);

Autenticação de Cliente - É o termo usado para descrever como o cliente pode comprovar sua identidade para outra pessoa, computador ou empresa;

Autoridade Certificadora -É a entidade responsável pela emissão do Certificado do cliente;

Browser - designado em português por **navegador**, é o programa que permite visualizar ou aceder a informação na Internet;

Certificação Digital - É a actividade de reconhecimento em meio electrónico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransmissível entre uma chave de criptografia, inserida em um Certificado Digital, o cliente e a Autoridade Certificadora;

Certificado Digital - É um conjunto de dados de computador que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia, o cliente e a Autoridade Certificadora;

Chave – Sequência de símbolos usados para codificar ou descodificar um arquivo;

Chave de Criptografia - É o valor numérico ou código que é aplicada para cifrar um determinado dado de computador;

Criptografia - É o embaralhamento dos dados referentes a um arquivo, e-mail ou transação. Desta forma, as informações são protegidas, antes de serem enviadas de um computador para outro, de maneira que somente o Cliente e o destinatário dos dados possam lê-los;

Directório - são entradas (registos) unicamente identificadas, onde cada entrada possui um ou mais atributos com uma estrutura hierárquica de dados;

Documento electrónico – sequência binária interpretada e visualizado por meio de um *software;*

Escalabilidade - É a propriedade de um sistema qualquer que lhe confere a capacidade de aumentar seu desempenho ou extensão quando são acrescentados recursos a esse sistema. Por exemplo, um sistema cujo desempenho aumenta com o acréscimo de hardware, proporcionalmente à capacidade acrescida, é chamado "sistema escalável";

Emissão de um Certificado Digital - É a actividade que se caracteriza pela geração de um Certificado Digital, a inclusão nesse dos dados de identificação do seu emissor (Autoridade Certificadora), do Cliente e da sua assinatura digital;

Exportação de um Certificado Digital - É a actividade de copiar, através do browser, um Certificado Digital instalado em determinado computador, para um disquete, CD-R, etc, permitindo a sua instalação em outro(s) computador(es). Esta acção somente é realizada mediante a utilização da senha pessoal de acesso;

Firmware - Programação em hardware; programa ou dados de computador que são armazenados permanentemente em um *chip* de memória de hardware, como uma ROM (*Read Only Memory*);

Internet – Rede mundial de computadores, constituída por várias redes que interligam entre si usando o protocolo TCP/IP;

Intranet – Rede baseada no protocolo TCP/IP que pertence a uma organização e que é acessível apenas aos membros da organização;

Interoperalidade - Habilidade de transferir e utilizar informações de maneira uniforme e eficiente entre várias organizações e sistemas de informação;

IP – *Internet Protocol.* Juntamente com o TCP, é o protocolo em que se baseia o funcionamento da Internet;

LDAP – Protocolo que permite o acesso à directórios, funciona sobre o TCP/IP;

OCSP – Protocolo que permite a verificação do estado de um certificado digital on-line;

Operador – usuário responsáveis pelo processamento da informação na AC ou AR;

Password - conhecida em português por **senha**, é constituída por uma única palavra ou sequência de caracteres, usada para autenticar uma identificação;

Protecção - Qualquer medida projectada para defender o equipamento e a informação de ataques;

RFC – *Request For Comments.* Documentos que definem normas e protocolos para a Internet, onde são feitas discussões e orientações de nível técnico;

Roteador - Dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede de computadores;

Scripts - é um tipo de programa (sequência de comandos) que executa comandos automaticamente, conforme o que for requisitado;

TCP/IP - *Transmission Control Protocol/Internet Protocol.* Protocolo (método) de comunicação entre computadores ligadas na Internet. É usado também em rede locais;

Texto claro – texto ou informação escrita de forma a permitir a qualquer ser humano uma fácil leitura. É o oposto de um texto criptográfico;

Topologia de rede – Distribuição geográfica ou lógica dos componentes ou equipamento que compõe a estrutura de uma rede;

Webmail – Sistema de e-mail acessível via Internet;

Website – Página de Internet que contém informações pessoais ou de uma organização.

Anexo 2: AVALIAÇÃO DE SOFTWARE PARA A IMPLEMENTAÇÃO DA PKI DA GOVNET

Esta secção visa apresentar alguns subsídios a serem consideração para a implementação do modelo proposto.

Independentemente da plataforma a ser adopta na implementação da PKI da GovNet as operações estão baseadas em dois pólos distintos (Módulo cliente e Módulo AC).

O **Módulo cliente** permite a interacção do usuário com a PKI e possui as seguintes funções: **Importação de certificados**; **Exportação do certificado**; **Assinatura e criptografia de documentos; Verificação de assinaturas** e **Requisição/Revogação de certificados na AC**.

O Módulo cliente será fornecido ao usuário em CDROM logo que for emitido o seu certificado para instalação no seu computador pessoal. Note-se que já existem vários programas no mercado preparados para usarem directamente os serviços de certificação.

O **Módulo AC** define o uso da infra-estrutura de chaves públicas por parte da AC. As funções são divididas em dois processos: **geração de certificados** e **revogação de certificados**. Estas funções são acessíveis exclusivamente à pessoas com permissão para operar o terminal da Autoridade Certificadora.

SOLUÇÃO DA MICROSOFT

O website http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod170.mspx (08 Jun 2005) disponibiliza um guia completo para a projecção e implementação de uma PKI no ambiente Microsoft Windows.

O sistema operacional da Microsoft possui muitos recursos de acesso a certificados e outras facilidades que ainda não foram implementadas noutros sistemas e é fácil de implementar.

Para construir uma AC aplicando a solução da Microsoft para além do sistema operativo windows, é necessário ter os produtos *Microsoft Information Server* e *Microsoft Certificate Server*, e para criar e executar os *scripts* seriam necessários o *ActiveX* e o *Visual Basic* (VBScript).

No entanto, esta solução acarreta custos elevados devido a aquisição de todos os componentes da solução e pagamento das licenças de utilização.

SOLUÇÕES *OPEN SOURCE*

OpenSSL

O *OpenSSL* foi desenvolvido pela Netscape com o objectivo de criar um canal seguro entre servidores web e navegadores de Internet. Segundo MARTINS (2004), o OpenSSL é dos pacotes mais conhecidos de criptografia.

O *OpenSSL* é a implementação do SSL e uma das formas de sua operação faz uso dos certificados digitais, por isso incluí funções e utilitários para a criação e gestão de certificados. Os utilitários são implementados na linguagem PERL.

A forma de gestão e armazenamento de certificados é realizada no formato de texto e cada certificado é guardado em um arquivo separado, o que torna difícil o processo de recuperação dos certificados.

O *OpenSSL* não implementa muitas das funcionalidades necessárias para uma PKI, por isso não pode ser considerado como um software para PKI, contudo é largamente aplicado como base para implementação de sistema de PKI.

A documentação e o software do *OpenSSL* está disponível no website oficial do projecto com o seguinte endereço: http://www.openssl.org/.

NewPKI

O *NewPKI* é um *software* para a implementação de uma PKI, baseado no *OpenSSL* e todos os dados são armazenados num banco de dados o que proporciona maior flexibilidade e recuperação dos dados mais eficiente. Este projecto é desenvolvido por um único indivíduo chamado Frédéric Giudicelli.

A implementação é feita em C++ o que possibilita a portabilidade do sistema para outras plataformas. Até ao momento esta solução funciona apenas com o SGDB MySQL, porém devido à camada de abstracção utilizada para acesso a base de dados, qualquer outro banco de dados pode ser usado.

A documentação e o software necessário para a implementação desta solução encontra-se disponível no website como seguinte: http://www.newpki.org/.

Vantagens:

- Visualização do *status* do processo de certificação via web e notificações por e-mail;
- Revogação de certificados e publicação via LCRs ou OCSP;
- Gestão de múltiplas ACs em único servidor;
- Suporte ao controle de políticas de certificado.

Desvantagens:

- Ausência de um grupo de desenvolvimento, o que processo de desenvolvimento lento;
- O armazenamento não pode ser feito numa base LDAP.

OpenCA

O projecto *OpenCA* é gerido por voluntários num processo colaborativo. Este projecto visa implementar uma interface para operações de emissão de certificados digitais para o sistema operacional GNU/Linux.

Este projecto está focalizado no usuário do software, que relata os problemas e envia sugestões apoiando deste modo a equipe de desenvolvimento.

Este projecto baseia-se no *OpenSSL*, *OpenLDAP*, *Apache* e PERL. Usa o *OpenSSL* para criptografia e emissão de certificados.

Os detalhes sobre a implementação e *software* do *OpenCA* podem ser obtidos no página do projecto com o endereço: http://www.openca.org/, onde pode ser obtida a documentação inicial e de instalação, assim como obter o próprio software.

Vantagens:

- Divulgação de certificados por LDAP;
- Suporta diversos tipos de bancos de dados (SGDB);
- Exportação de usuários e certificados;
- Suporta à criptografia e geração de certificados fornecidos pelo OpenSSL;
- Usa a interface web para a sua gestão.

Desvantagens:

- Não suporta backup da chave privada;
- Não pode ser usado na plataforma win32 devido às permissões dos usuários e grupos;
- Dificuldade de modificação do código devido a grande fragmentação do mesmo;
- Divulgação da situação dos certificados realizada apenas por LCRs.

IDX-PKI

O projecto IDX-PKI foi desenvolvido pela companhia francesa IdealX que o publica e mantém.

O IDX-PKI usa Perl, PHP, C, *shellscripts*, bem como alguns utilitários GNU e já está pronta para o uso diário e continua a ser aperfeiçoado. Entre outras coisas está planeada a capacidade de comunicação segura entre diferentes PKIs e permite a escolha do repositório, seja banco de dados, LDAP ou sistema de arquivos.

Os detalhes deste projecto e o software podem ser obtidos no website com o seguinte endereço: http://idx-pki.idealx.org/index.en.html.

Vantagens:

- Armazenamento de certificados usando LDAP ou banco de dados SQL;
- Flexibilidade na modificação do código
- Divulgação dos certificados usando LCRs ou OCSP;
- Suporte às empresas que desejarem adoptar o produto;

Desvantagens:

- Suporta apenas os sistema operacionais *unix-like* (devido ao uso de *shellscripts* e utilitário da GNU)
- Dificuldade de instalação devido à dependência de módulos do Perl;
- Falta de documentação;
- Modularidade excessiva, possui pequenos módulos em linguagens diversas.

SOLUÇÕES COMERCIAIS

As soluções comerciais são suportadas por empresas que comercializam soluções PKI e em geral vendem certificados por um período determinado e soluções de software para a gestão de certificados. Segundo MARTINS (2004), o que se encontra em muitos países são empresas que comercializam soluções que fazem uso de certificados digitais e consequentemente dependem de uma PKI já estabelecida.

Normalmente esta empresas enquadram-se na estrutura da PKI como ACs credenciadas pela AC-Raiz ou prestadoras de serviços .

SOLUÇÃO SUGERIDA

Pela avaliação realizada é sugerida a solução *NewPKI* os pontos considerados foram:

- Projecto devidamente documentado;
- Aderência aos padrões existentes;
- Funcionalidades e independência à plataforma de implementação;
- flexibilidade de alteração e simplicidade na pesquisa;
- solução não proprietária.

Outro aspecto relevante a destacar é referente a viabilidade do uso da solução *open souce* (código livre). Devido ao alto custo das soluções proprietárias e o facto das versões gratuitas serem de código aberto, oferecendo possibilidade do ajuste da aplicação as necessidade, maior segurança e capacidade de ser auditado. Existe actualmente uma tendência das empresas e principalmente de alguns governos de migrar do software proprietário para as versões livres. Estas considerações também motivaram a selecção da solução.

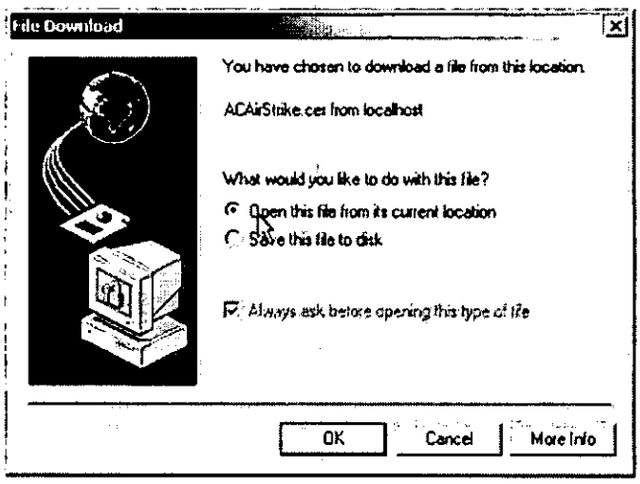
Em anexo ao presente trabalho é apresentada a interface web da NewPKI, para mostrar o funcionamento desta solução no seu ambiente real.

Anexo 3: INSTALAÇÃO DO CERTIFICADO DIGITAL NO *BROWSER*

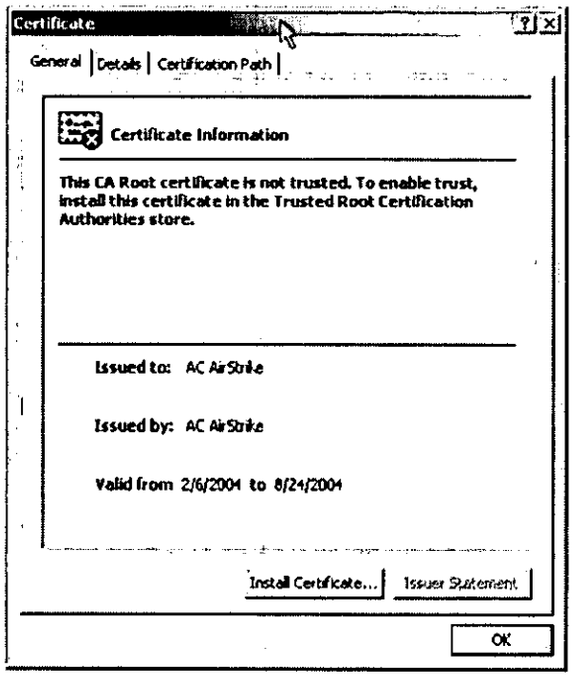
O primeiro passo a realizar para a instalação do certificado no *browser* é a descarga (*download*) do certificado da Autoridade Certificadora Raiz na página web da PKI da GovNet .

O exemplo que segue, foi extraído de (MARTINS, 2004) mostra a instalação do certificado da ACAirtrike.

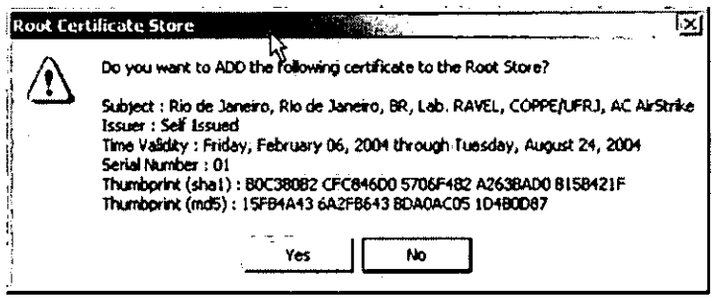
Geralmente, ao clicar o link de *download* aparece a janela apresentada abaixo, onde deve ser seleccionada a opção *open* para abrir o arquivo, como mostra a figura que segue.



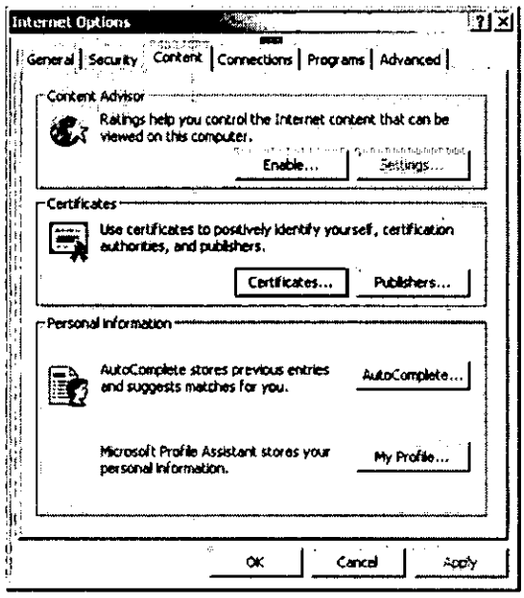
Em seguida, na barra inferior da janela que surge existe a opção *install Certificate* (Instalar o Certificado).



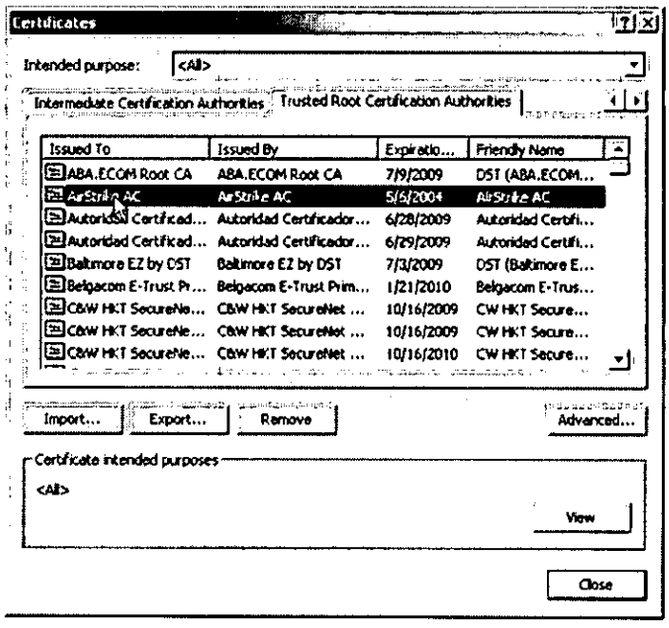
O processo termina com a janela seguinte, solicitando a confirmação dos dados do certificado a instalar no *browser,* onde deve se pressionado botão YES.



Para confirmar a correcta instalação basta navegar pelos menus ***Tools*** => ***Internet Options*** até a janela da figura abaixo.



Utilizando a opção ***Certificates*** é mostrada a janela que segue e deve ser seleccionado o último guia, para exibir a lista das AC cujos os certificados foram instalados, o nome da AC instalada deverá constar na lista.



O certificado da AirStrike AC está instalado como mostra a figura acima.

Anexo 4: Requisitos de Software e Hardware

Requisitos de Software para as ACs

- Linux
- Apache 1.3.23
- PHP 4
- MySQL versão superior a 3.23.49
- LDAP
- NewPKI
- Antivírus
- Antitrojans

  - O sistema operacional deve ser instalado em sua forma mais básica.
  - Serviços do sistema operacional como Telnet, FTP ou qualquer tipo de acesso remoto não deverão ser habilitados.
  - Deverão ser activados todos os serviços de auditoria relativos a gravação de logs.

Requisitos de Hardware para as ACs

1. Servidores das ACs

Os servidores da AC-Raiz, AC e AR devem possuir no mínimo os seguintes requisitos:

- Pentium IV 2.0GHz
- 512 MB de memória RAM
- Discos Rígidos: 2x73 GB
- Drive de disquete 1.44
- Drive de CD-ROM/DVD
- Monitor
- Teclado
- Mouse
- Porta USB
- Possuir fontes de alimentação de energia e ventilação redundantes.
- Possuir gabinete com característica para montagem em *Rack* padrão 19" (dezenove polegadas), altura máxima de 2U's;

Interfaces de Rede:

Quantidade: 2 (duas)

- Taxa de Transferência: 10/100/1000 Mbps (dez, cem e mil megabits por segundo);
- Padrão : IEEE 802.3/802.3u/802.3ab;
- Possuir conexão via par trançado UTP Categoria 6 por intermédio de conectores padrão RJ-45;

Interface de Rede Gigabit Ethernet:

Quantidade: 3 (três);

- Padrões: 802.3z e 802.1Q, multiple VLANs
- velocidade de 1000 Mbps (um mil megabits por segundo) ou 1 Gbps (um gigabit por segundo);
- Possuir tecnologia de balanceamento de carga;

- O servidor deverá ser acompanhado de software de configuração inicial (instalação), permitindo ajustes dos parâmetros de hardware e a instalação simplificada do sistema operacional da solução.
- Ser acompanhada de software/utilitário e *driver*s para instalação do periférico no sistema, compatível com o Linux.

2. Hardware Security Module para AC

O Hardware Security Module (HSM) pode ser interno ou externo. O HSM interno é acoplado na barramento PCI da placa mão do servidor da AC,enquanto que HSM externo é conectado na rede interna e é acedido via TCP/IP.

Os requisitos da HSM são seguintes:

- Autenticação para acesso ao HSM via *smart cards*
- Suporte a certificados X.509 v3 e pedidos de certificados via PKCS#10
- Interfaces Padrão para criptografia em tokens (PKCS#11)
- Customizável
- Possível *upgrade* de *firmware* com HSM em operação
- Relógio interno de tempo real
- Gerador de números randômicos por hardware
- Suporte de algoritmos assimétricos: RSA, DAS, Diffie-Hellmann
- Suporte de algoritmos simétricos: DES, DES3, IDEA, RC2, RC4
- Autenticação de mensagens e *hash*: SHA-1, MD-2, MD-5, RIPEMD-128, HMAC-MD, DES-MAC, AES
- Suporte aos diferentes padrões de APIs criptográficas existentes
- Memória segura com bateria para armazenamento de chaves (1Mbyte)
- Acesso via TCP/IP em rede *Ethernet* (HSM externo)

3. Repositório de Certificados e Lista de Certificados Revogados

Processadores:

Quantidade: 2 (dois)

- modelo padrão Intel Xeon, 3,6GHz;
- Suporte ao sistema operacional Linux.

Memória RAM:

- Capacidade mínima instalada: 6 GB (seis gigabytes);

Fonte de Alimentação

Quantidade: 2 (duas), funcionamento de forma redundante;

Placa controladora de vídeo Padrão: SVGA, Memória mínima de vídeo, não compartilhada de 8 MB (oito megabytes);

Controlador de discos:

- Padrão: Ultra3 SCSI ou superior;
- Implementar RAID nos níveis 0,1,5 e 0+1 por hardware.

Unidade de Discos Rígidos (HD):

- Quantidade: 5 (cinco) unidades de mesma marca e modelo;
- Padrão: Ultra3 SCSI (Ultra320) ou superior;
- Capacidade mínima : 146 GB (cento e quarenta e seis gigabytes) em 1 (um) disco;
- Capacidade mínima : 73 GB (setenta e três gigabytes)nos outros 4 discos;

Unidade de Disco flexível (Disquete)

Interfaces de Rede:

Quantidade: 2 (duas)

- Taxa de Transferência: 10/100/1000 Mbps (dez, cem e mil megabits por segundo);
- Padrão : IEEE 802.3/802.3u/802.3ab;
- Possuir tecnologia de balanceamento de carga;

Interface de Rede Gigabit Ethernet:

Quantidade: 3 (três);

- Padrões: 802.3z e 802.1Q, multiple VLANs com velocidade de 1000 Mbps (um mil megabits por segundo) ou 1 Gbps (um gigabit por segundo);
- Possuir tecnologia de balanceamento de carga;

Porta PS/2 para *Mouse*

Porta PS/2 para Teclado

Gabinete:

- Possuir característica para montagem em *Rack* padrão 19" (dezenove polegadas);

Sistema Operacional:

- O Servidor deverá ser fornecido com o sistema operacional Linux instalado
- A versão do sistema operacional Linux, deve ser a mais recente
- Possuir suporte em inglês ou português;
- Manuais em inglês ou português;
- O sistema operacional deve possuir certificado de registro e garantia.

4. Backup

Requisitos mínimos obrigatórios:

Quantidade: 1 (uma unidade);

- Ser um sistema automatizado de fitas cartucho;
- Possuir capacidade de armazenar, no mínimo, 10 (dez) cartuchos do tipo LTO;
- Cada cartucho deverá possuir um mínimo de 200 GB (duzentos gigabytes) de capacidade de armazenamento
- Possuir a capacidade de manutenção e substituição de cartuchos, sem interrupção dos processos de backup ou *restore* em curso;
- Possuir sistema de leitura de código de barra;
- Possibilitar administração remota via web;
- Possuir painel de controle para monitoramento e diagnóstico;
- Possuir compatibilidade com os sistemas operacionais: Windows NT 4.0, Windows 2000, Windows 2003, Linux e Sun Solaris;
- Deve suportar o software de backup Veritas

5. Requisitos do USB Token

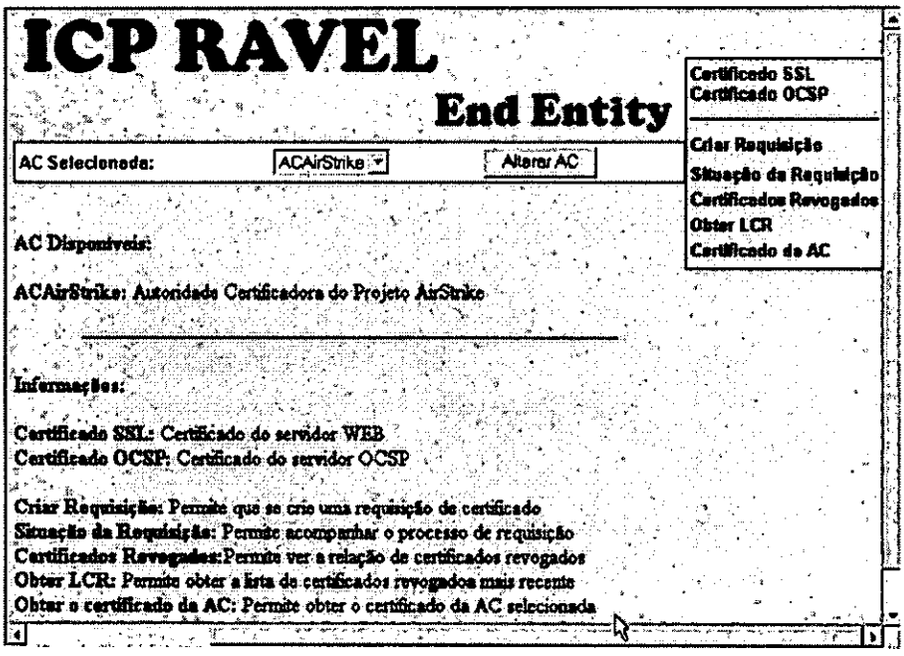
O USB Token deverá conter a chave privada e o certificado digital do usuário final, permitindo que o usuário possa se autenticar ou assinar digitalmente quanto for requerido em qualquer computador. Deve possui as seguintes características:

- Atender especificamente às necessidades da PKI e assinatura digital, permitindo a geração segura de chave criptográfica em hardware
- Memória protegida de 8Kb para armazenamento do certificado e da chave privada

- Controlador USB compatível com USB 1.1 e 2.0
- Suportar o *software* criptográfico RSA de 1024 bits
- Executar algoritmos criptográficos DES, 3DES, RC2, RC4 e RC5
- Permitir conexão directa na porta USB sem necessidade de interface intermediário para leitura
- Possuir indicador luminoso de estado do dispositivo
- Suporte aos diferentes padrões de APIs criptográficas existentes
- Interfaces Padrão PKCS#11

Anexo 5: INTERFACE WEB DA SOLUÇÃO SUGERIDA PARA A PKI DA GOVNET

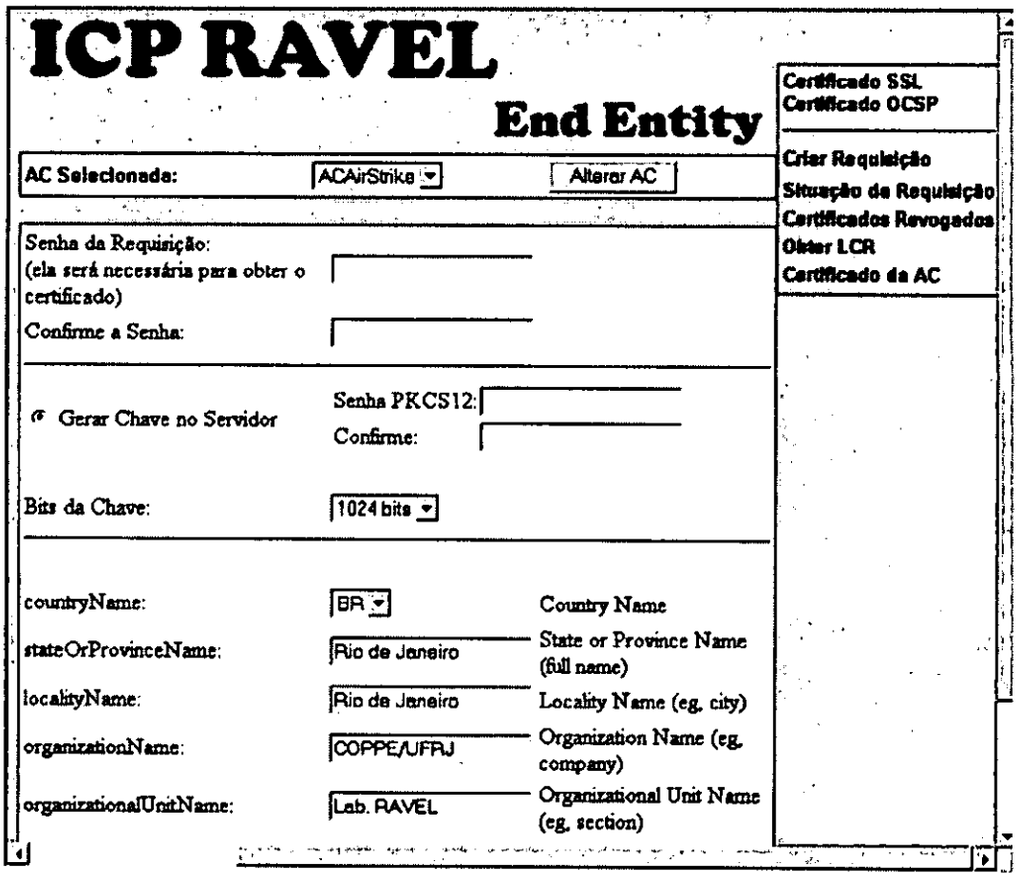
A Interface Web da solução é escrita em PHP que provê as funcionalidades da PKI. A interface apresentada em seguida ilustra o modo de interacção do usuário final com a PKI, foi extraídas do sistema AirStrike (MARTINS, 2004).



Tela inicial da interface web da NewPKI

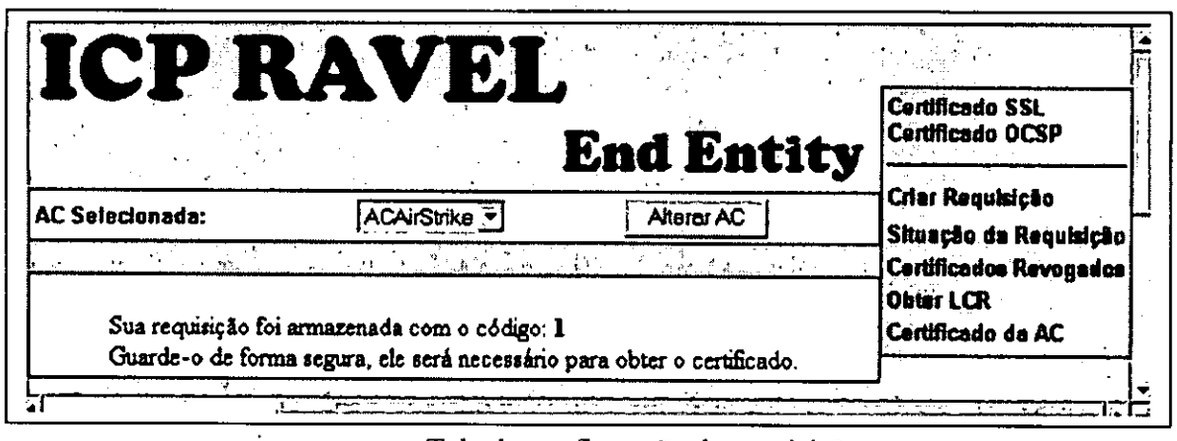
Esta tela permite seleccionar uma AC e contém um menú com várias opções que permitem:

- Requisição de certificados digitais;
- Acompanhar a situação da requisição após a solicitação;
- Obter a Lista de Certificados Revogados; e
- Obter o certificado da AC seleccionada.

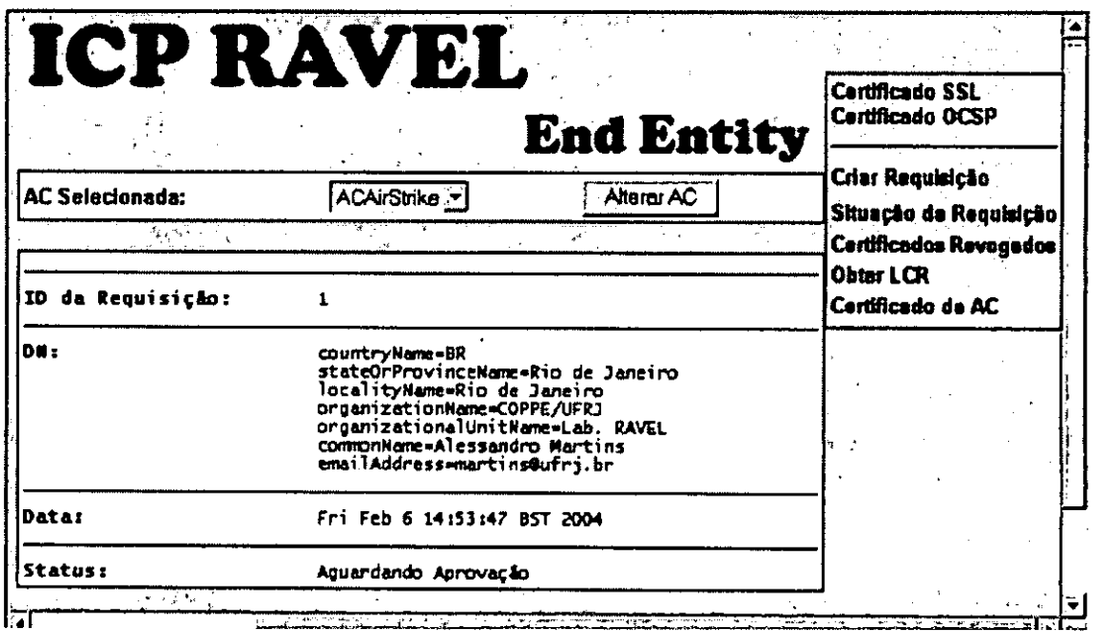


Tela com o Formulário de requisição de certificado

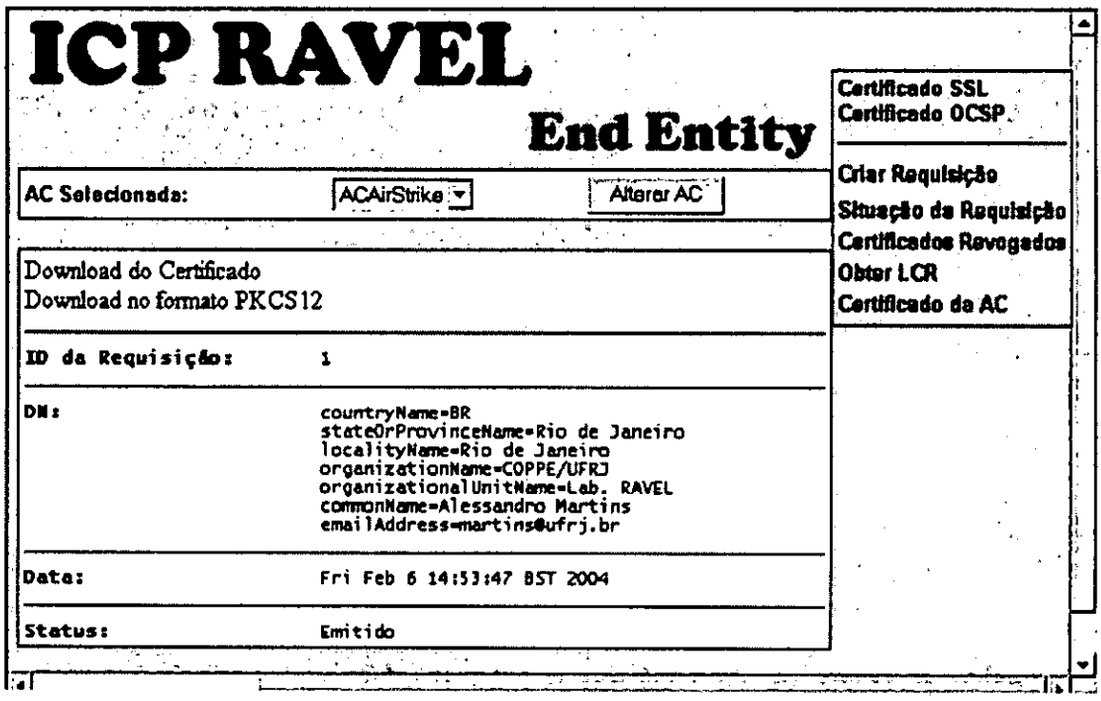
Esta tela permite realizar a requisição de um certificado digital, através da interface web e gerar a chave no servidor.



Tela de confirmação da requisição



Tela com a informação sobre o situação do processo de requisição



Tela final do processo de requisição, confirmando a emissão do certificado.