UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Luciano Ignaczak

Um Novo Modelo de Infra-estrutura de Chaves Públicas para Uso no Brasil Utilizando Aplicativos com o Código Fonte Aberto

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.
Orientador
custodio@inf.ufsc.br

Florianópolis, Maio de 2002

Um Novo Modelo de Infra-estrutura de Chaves Públicas para Uso no Brasil Utilizando Aplicativos com o Código Fonte Aberto

Luciano Ignaczak

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação, área de concentração Segurança em Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Prof. Fernando Ostuni Gauthier, Dr.

Coordenador do Curso

gauthier@inf.ufsc.br

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.

Orientador

custodio@inf.ufsc.br

Prof. Luiz Carlos Zancanella, Dr.

zancanell@inf.ufsc.br

Prof. Jeroen van de Graaf, Dr.

jvdg@cenapad.ufmg.br

Prof. Carlos Roberto De Rolt, Dr.

rolt@datalan.com.br

”Nada em todo mundo é mais perigoso que a ignorância sincera e a estupidez consciente”. Martin Luther King Jr.

Para meus pais João Carlos Ignaczak e Elcida Maria Mezzomo Ignaczak que tornaram possível a realização deste trabalho.

Agradecimentos

Gostaria de agradecer a todos os meus colegas do LabSEC que contribuíram com o trabalho. São eles: Júlio da Silva Dias, Augusto Jun Devegili, Luciana Schmitz, Jean Everson Martina, Carlos Eduardo Silva, Everton Schonardie Pasqual e Roberto Samarone Santos Araújo.

Agradeço também aos meus amigos, que sempre estiveram ao meu lado durante mais essa jornada. São eles: João Carlos Vieira, Fabiano Goellner dos Santos, Marcelo Carlomagno Carlos, Taís Biavatti, Gislaine Parra, Eliane Rodrigues Fogaça e Osvaldo Cardoso.

Um agradecimento especial para o meu orientador Prof. Dr. Ricardo Felipe Custódio por todo o tempo dispensado para aprimorar meu aprendizado e deixar-me apto a escrever esta dissertação.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

AA	Autoridade de Aviso
AC	Autoridade Certificadora
ACC	AC Central
AC-Raiz	AC Raiz
AD	Autoridade Datação
AGP	Autoridade de Gerenciamento de Políticas
AH	Authentication Header
AR	Autoridade de Registro
ARL	Autoridade de Registro Local
DPC	Declaração de Práticas de Certificação
DSA	Digital Signature Algorithm
ESP	Encapsulating Security Payload
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
ICP	Infra-Estrutura de Chaves Públicas
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	IP Security
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LabSEC	Laboratório de Segurança em Computação
LAR	Lista de Autoridades Revogadas

LCR	Lista de Certificados Revogados
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extension
MP	Medida Provisória
NSA	National Security Agency
OCSP	Online Certificate Status Protocol
OSI	Open Systems Interconnection
PC	Políticas de Certificação
PDDE	Protocolizadora Digital de Documentos Eletrônicos
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standards
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman - Nome dos criadores
SET	Secure Electronic Transaction
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
S/MIME	Secure/Multipurpose Internet Mail Extension
TCP	Transfer Control Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WTLS	Wireless Transport Layer Security

Resumo

Este trabalho propõe a adoção de um novo modelo - com a inclusão de novas características - de Infra-estrutura de Chaves Públicas para o Brasil considerando a experiência adquirida na implantação da ICP-UFSC. A partir de um estudo aprofundado dos tipos de modelos existentes e de modelos que estão sendo implantados em outros países, juntamente com a constatação de que o modelo escolhido pelo governo brasileiro necessita de aprimoramentos, foi escolhido um novo modelo com o objetivo de atender, da melhor forma possível, as necessidades nacionais. O modelo proposto visa garantir a independência de todos os órgãos do governo, assim como das empresas privadas nacionais e internacionais que utilizarão os serviços da Infra-estrutura de Chaves Públicas brasileira. O trabalho também descreve novos componentes e características que uma ICP deve incorporar a sua estrutura para oferecer novos serviços para seus usuários, além de aperfeiçoar serviços existentes. Outro ponto abordado é a adoção de uma nova metodologia envolvendo o uso de aplicativos com código fonte aberto, visando garantir um nível de segurança mais alto para seus usuários.

Palavras Chaves: Infra-estrutura de Chaves Públicas, Segurança em Redes, Certificados Digitais.

Abstract

This work deals with the adoption of a new Public Key Infrastructure (PKI) model - which includes a new set of characteristics - for Brazil. The model is based on the experience gained while implementing the UFSC PKI. Besides analyzing PKI models adopted elsewhere, a detailed study was carried out within existing models. This study showed that the PKI model chosen by Brazilian government needs improvement. Therefore, a new model was proposed to meet the national needs. This model should guarantee the independence of all Brazil federal agencies, as well as national and international private companies which will use the services of the Brazilian PKI. This work also reveals new components and characteristics that a PKI must incorporate into its architecture in order to offer new services and improve the existing ones. In addition, the adoption of open source softwares methodology will insure a higher level of security of the PKI users.

Keywords: Public Keys Infrastructure, Network Security, Digital Certificates.

Capítulo 1

Introdução

Atualmente, é perceptível o contínuo aumento no número de pessoas que acessam a Internet. Este aumento tem demonstrado a necessidade do surgimento de novos serviços, visto que os disponíveis não possuem características de escalabilidade para atender a essa crescente demanda. Além disso, os serviços existentes estão sofrendo constantes modificações para adequarem-se às novas tecnologias e exigências de qualidade. Esse crescimento aliado ao aprimoramento, tornam a competição entre empresas que prestam o mesmo tipo de serviço cada vez mais acirrada. Para essas empresas conseguirem destacar-se e alcançar novos clientes, elas devem procurar diferenciais que as outras ainda não possuam. Um diferencial é a segurança dos sistemas, dos dados da empresa e dos seus clientes.

A segurança tem uma importância maior para empresas que possuem serviços voltados para a área do comércio eletrônico. Pois esses serviços exigem a execução de transações que, normalmente, envolvem informações sensíveis, tais como números de cartões de créditos ou dados bancários das entidades envolvidas. Acredita-se que muitas empresas desse ramo ainda não atingiram o número de clientes esperado. Isto deve-se, em parte, ao receio que grande parte das pessoas tem de enviar dados privativos através da Internet. Esse receio é enfatizado pelos inúmeros problemas nos sistemas de segurança das empresas que são noticiados todos os dias[GEN 01].

A implementação de uma Infra-estrutura de Chaves Públicas (ICP) in-

tegrada à estrutura da empresa é uma excelente solução para resolver os problemas de segurança [BIC 00]. Uma ICP é responsável pela emissão e gerenciamento de certificados digitais. Este possui serviços de forma a garantir os requisitos de segurança: identificação, integridade e sigilo.

Normalmente, as empresas que utilizam esse tipo de solução têem obtido bons resultados. Mesmo as empresas que não tenham condições financeiras ou técnicas para implantar uma ICP própria, podem resolver seus problemas de segurança contratando serviços de outras ICP.

Recentemente, o governo brasileiro instituiu a Infra-estrutura de Chaves Públicas, denominada ICP-Brasil. Com isso, o governo pretende incentivar o uso de documentos eletrônicos para troca de informações de forma a melhorar a qualidade de seus serviços para o cidadão.

1.1 Objetivos

1.1.1 Objetivo Geral

O objetivo geral da dissertação é propor um modelo de Infra-estrutura de Chaves Públicas para o Brasil, considerando a estrutura organizacional dos poderes Judiciário, Legislativo e Executivo, assegurando a independência entre eles. Além disso, para garantir a segurança e a transparência da infra-estrutura, propõe-se a utilização de aplicativos com código fonte aberto.

1.1.2 Objetivos Específicos

- Apresentar a recomendação X.509 do ITU-T;
- Levantamento da legislação brasileira sobre assinatura digital e documentos eletrônicos;
- Descrever os componentes necessários a uma ICP;
- Análise e crítica à ICP-Brasil;

- Descrição das vantagens da utilização de softwares com código fonte aberto;
- Levantamento detalhado dos modelos de ICP de diferentes países;
- Propor um modelo geral para o Brasil considerando os novos componentes e necessidades levantadas.

1.2 Motivação

Uma das grandes vantagens do uso da Internet foi a aceleração do processo de disseminação das informações, que tornou possível o acesso à informação de maneira mais rápida e eficiente.

Os aplicativos de código aberto começaram a ganhar espaço no mercado no momento que as empresas e as pessoas perceberam que eles trazem uma maior confiança para seus usuários. Isso é possível, em princípio, pela possibilidade de compreensão de todos os passos executados durante seu processamento.

Por causa dessa confiança, o uso desse tipo de aplicativo é indicado, principalmente, na área de segurança. Empresas que trabalham nesta área não deveriam usar aplicativos que não possuam seu código fonte disponível. Pois não há garantias que programas com código fonte fechado executem somente o que dizem executar.

A Infra-estrutura de Chave Públicas do Brasil (ICP-Brasil) é um dos projetos sobre segurança da informação mais importante no Brasil nos últimos anos. Por causa disso o modelo de ICP proposto está causando muitas discussões por parte do governo e outras organizações. Grande parte dos problemas estão sendo causados porque os três poderes serão submetidos às políticas de uma única Autoridade Certificadora Raiz (AC Raiz), sendo controlada por um comitê formado, em sua maioria, por membros do poder executivo [BRA]. Através deste documento propõe-se um novo modelo de ICP para ser utilizado no Brasil, buscando acabar com a dependência causada pelo modelo atual.

1.3 Metodologia e Ferramentas

Para a realização desta dissertação, foi realizada uma ampla pesquisa bibliográfica, baseada em livros, artigos científicos e dissertações de mestrado.

Para a realização da pesquisa bibliográfica foram adquiridos os principais livros conhecidos sobre ”Infra-estrutura de Chaves Públicas”publicados até dezembro de 2001.

Também foram pesquisados os artigos existentes sobre o assunto, nas principais revistas da área de segurança em computação.

Para garantir a proposta de um tema atual, foram acompanhadas as alterações ocorridas na legislação brasileira. Para isso foram visitados regularmente sites do governo, além da leitura de relatórios técnicos.

O LabSEC também foi responsável pela implantação de uma Infra-estrutura de Chaves Públicas dentro da Universidade Federal de Santa Catarina (UFSC). Desta forma foi possível formar uma base de conhecimento, através de experiências práticas, que agregou um grande valor no momento de propor um novo modelo de ICP.

1.4 Conteúdo do Trabalho

O capítulo 2 descreve os conceitos de criptografia, além de todos os conceitos necessários para a criação da assinatura digital de um documento eletrônico. O capítulo 3 descreve os principais componentes necessários para a implantação de uma ICP. O capítulo 4 apresenta uma revisão do protocolo X.509, teorizando certificados digitais e listas de certificados revogados. O capítulo 5 apresenta o conceito do que é um aplicativo com código fonte aberto e suas vantagens em relação a outros tipos de aplicativos. O capítulo 6 abrange o modelo de ICP definido pela ICP-Brasil e outros modelos existentes. O capítulo 7 aborda protocolos que fornecem suporte para certificados digitais. Finalmente, o capítulo 8 descreve um novo modelo, com novas características, que possui reais vantagens sobre o modelo atualmente proposto pelo governo brasileiro.

Capítulo 2

Fundamentos Criptográficos

2.1 Introdução

Este capítulo aborda as técnicas de criptografia e os serviços por ela oferecidos. A criptografia é uma das ferramentas mais adequadas para garantir a segurança de dados e comunicações. O capítulo descreve, também, funções e protocolos que definem padrões através do uso da criptografia.

O capítulo também abrange os diferentes mecanismos existentes para autenticação e descreve como é realizada a criação da assinatura digital de um documento eletrônico.

A seção 2.2 conceitua a criptografia e seus serviços. A seção 2.3 aborda as características da criptografia simétrica. A seção 2.4 comenta as vantagens do uso de criptografia assimétrica. A seção 2.5 descreve as características de uma função resumo. A seção 2.6 demonstra os tipos de autenticações possíveis. A seção 2.7 conceitua assinatura digital. Finalmente, a seção 2.8 aborda os padrões de criptografia de chave pública.

2.2 Criptografia

Historicamente o principal objetivo da criptografia era possibilitar a comunicação segura entre duas partes, através de um canal não seguro, de tal forma que

uma terceira parte não consiga entender o conteúdo que está sendo transmitido[STI 95].

A criptografia provê recursos para garantir os seguintes serviços:

Autenticação Garante a identificação do indivíduo responsável por uma transação;

Confidencialidade Garante o sigilo de uma mensagem. Ninguém que não possua autorização acessará o conteúdo de uma mensagem;

Irretratabilidade Impossibilita a negação do envio de uma mensagem por seu autor.

2.3 Criptografia Simétrica

A criptografia simétrica foi a primeira forma conhecida para ocultação de dados. Uma técnica de criptografia simétrica foi utilizada por *Julius Caesar* para enviar mensagens seguras para seus exércitos [STA 99].

A principal característica da criptografia simétrica é a utilização de somente uma chave para autenticar e garantir a confidencialidade de uma mensagem. Um exemplo de criptografia usando chaves simétricas é mostrado na figura 2.1.

A chave é gerada pelo emissor da mensagem. Com ela cifra-se o texto que depois é transmitido para uma ou mais pessoas. A criptografia simétrica necessita que todos os atores envolvidos no processo tenham conhecimento da chave. Um grande problema disto é garantir o compartilhamento deste segredo de forma confiável. Se o segredo for compartilhado entre mais de duas pessoas surge outro problema: a autenticação não pode mais ser assegurada. Qualquer um poderá cifrar uma mensagem usando a chave de conhecimento do grupo, alegando ser outra pessoa que possua conhecimento da mesma chave.

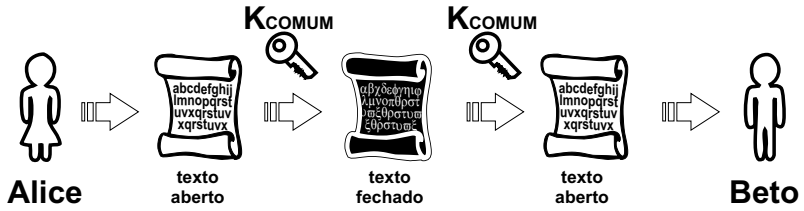

Figura 2.1: Alice de posse de um texto aberto cifra-o, utilizando um algoritmo de chave simétrica, com a chave K_{comum} obtendo um texto fechado. Beto de posse do texto cifrado utiliza a mesma chave K_{comum} para decifrá-lo e lê-lo.

2.4 Criptografia Assimétrica

A criptografia assimétrica ou de chave pública utiliza, normalmente, duas chaves diferentes, mas relacionadas. Sendo uma privada e outra pública. Um texto cifrado com uma das chaves pode somente ser decifrado utilizando a outra.

A garantia da confiança está no fato de que cada usuário deverá gerar seu próprio par de chaves. A chave privada deve ser mantida em segredo. Esta chave não pode ser utilizada por ninguém, exceto pela pessoa a qual ela pertence. A chave pública, ao contrário, deve ser disponibilizada para ser utilizada por qualquer indivíduo ou aplicação.

A criptografia assimétrica permite a utilização de dois tipos de serviços. O primeiro é a assinatura digital que é criada através do uso da chave privada e sua verificação é feita utilizando a chave pública.

O outro serviço é o sigilo. Ele utiliza a chave pública do destinatário para cifrar uma mensagem, o qual deve utilizar sua chave privada para a decifrá-la. A função de sigilo é ilustrada na figura 2.2.

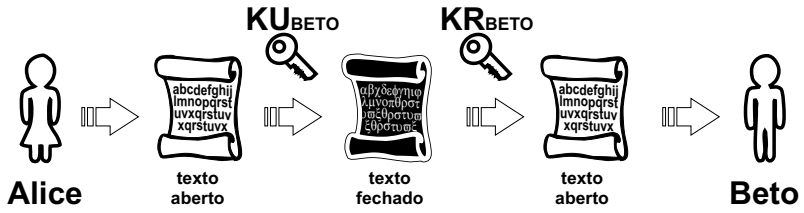

Figura 2.2: Alice cifra o texto que ela deseja enviar para Beto usando a chave pública(KU_Beto) do mesmo. Após o recebimento do texto fechado Beto deverá torná-lo legível, para isto ele utilizará sua chave privada(KR_Beto) para decifrá-lo.

2.5 Função Resumo

Função Resumo é uma função que recebe como entrada um conjunto de bits de qualquer tamanho e produz um resultado de tamanho fixo. O tamanho da saída varia de acordo com o algoritmo usado. O propósito de uma função resumo é produzir uma ”impressão digital” da mensagem [STA 99].

Funções Resumo são funções de sentido único, ou seja, a mensagem não pode ser determinada através do seu resumo. Outra característica desse tipo de função é que seu resultado deve ser muito diferente se apenas um bit de uma mensagem for alterado.

Com o resultado gerado por uma Função Resumo é possível garantir a integridade de uma mensagem, pois se alguma parte dela for alterada, quando a Função Resumo for aplicada novamente na mensagem, seu resultado será diferente. Utilizando uma Função Resumo é possível detectar qualquer alteração em uma mensagem, mesmo sendo apenas a modificação de uma letra.

2.6 Autenticação

A autenticação provê a garantia de que as entidades envolvidas em uma transação são quem elas dizem ser. Estas entidades podem ser pessoas ou dispositivos [FEG 99].

Uma autenticação pode ser feita considerando os seguintes fatores:

Algo que você sabe A autenticação é feita através de algum conhecimento específico do indivíduo.Este conhecimento pode ser uma senha ou um número de identificação pessoal.

Algo que você tem A entidade é identificada através da posse de algo, o objeto pode ser, por exemplo, um disquete ou um smart card com a chave privada armazenada.

Algo que você é Ele utiliza alguma medida biométrica para identificação. Por exemplo a impressão digital ou a íris.

Onde você está Este tipo de autenticação leva em consideração a posição geográfica do indivíduo no momento da autenticação. A verificação deste tipo de autenticação pode ser feita utilizando, por exemplo, algo semelhante a um dispositivo de Global Positioning System (GPS).

Momento da Autenticação Esta autenticação baseia-se na validação da data e hora que o usuário está autenticando-se perante um sistema. A data e hora serão atribuídas por uma protocolizadora digital. Assim não será possível burlar o sistema porque somente um horário assinado por um dispositivo válido será validado.

Presença de testemunha A autenticação é realizada apenas com a presença de uma ou mais testemunhas. Este tipo de autenticação possui uma segurança muito grande devido à necessidade de duas ou mais pessoas autenticarem-se no sistema. Esta autenticação resolve o problema do comprometimento da chave privada da pessoa que vai autenticar-se perante o sistema, pois a presença da testemunha cancelará a operação.

A autenticação também pode ser feita através da combinação de dois ou mais dos fatores acima citados. Esta forma de autenticação permite um acréscimo no nível de segurança. Por exemplo, a autenticação pode ser feita digitando uma senha, junto com a verificação da impressão digital do indivíduo.

2.7 Assinatura Digital

Uma assinatura digital é um conjunto de dados em forma eletrônica, os quais são anexados ou logicamente associados com outros dados em forma eletrônica. Estes dois conjuntos de dados servem como método de autenticação[Gui 00].

A assinatura digital é utilizada para verificar a autenticidade e a integridade de dados. Para a criação da assinatura digital de uma mensagem o indivíduo deve utilizar sua chave privada.

Para gerar uma assinatura digital, primeiro é executado o processo para criação do resumo da mensagem. Após, o resumo é cifrado utilizando a chave privada do assinante. O resultado é a assinatura digital da mensagem.

O processo para verificação da assinatura digital é realizado da seguinte forma: no momento que o usuário recebe a mensagem, ele cria o seu resumo. Criado o resumo da mensagem, ele decifra o resumo que foi enviado juntamente com a mensagem, utilizando a chave pública do emissor. Se o resultado da nova função resumo for idêntico ao resumo decifrado, é possível garantir a integridade da mensagem e assegurar que os dados foram assinados pela chave privada correspondente àquela chave pública. Este processo é ilustrado na figura 2.3.

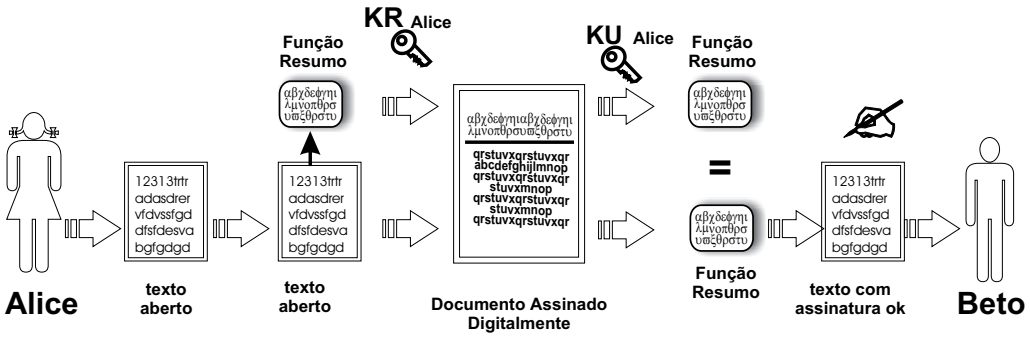

Figura 2.3: Para criar a assinatura digital de um documento, Alice executa a função resumo dele e cifra o resultado com sua chave privada. O resumo cifrado é enviado para Beto juntamente com o documento. Beto decifra o resumo com a chave pública de Alice, executa novamente a Função Resumo do documento e compara os dois resultados. Se forem iguais a assinatura é válida.

2.7.1 RSA

O RSA, criado por Ron Rivest, Adi Shamir e Leonard Adleman em 1976, foi o primeiro algoritmo de sucesso utilizado tanto para cifrar dados como para assinatura digital. O RSA é certamente o algoritmo mais popular e, conseqüentemente, o que possui o maior número de aplicações compatíveis.

A segurança desse algoritmo é baseada na dificuldade de fatorar um número muito grande. Porém existem dois fatores que podem ameaçar este tipo segurança: o constante crescimento do poder de processamento dos computadores e as melhorias nos algoritmos de fatoração [STA 99].

2.7.2 DSA

O algoritmo de assinatura digital (Digital Signature Algorithm - DSA) foi proposto, em agosto de 1991, pelo Instituto Nacional de Padrões e Tecnologia Norte Americano (NIST) para ser utilizado como o padrão para assinatura digital. O DSA é uma variação de outro algoritmo para assinatura digital, o ElGamal [SCH 96].

A proposta gerou muitas críticas por partes de empresas da área de segurança, devido a problemas encontrados no algoritmo sugerido. O DSA havia sido desenvolvido pela Agência de Segurança Nacional do Estados Unidos (NSA) e isto trazia a desconfiança que poderiam haver atalhos para que a agência pudesse quebrar uma chave com facilidade. Aliado a isto, a NSA sugeriu inicialmente a utilização de uma chave de 512 bits, cujo tamanho é considerado pequeno para os padrões atuais. Em vista disso, a NSA possibilitou a geração de chaves com 1024 bits.

2.8 Padrões de Criptografia de Chaves Públicas

A Empresa RSA Security em cooperação com desenvolvedores definiu uma série de padrões para o uso da criptografia de chave pública. Eles são denominados Public Key Cryptography Standards (PKCS). Atualmente, existem 15 padrões já definidos. A tabela 2.1 lista todos os padrões e suas definições.

Tabela 2.1: A tabela acima lista os padrões de criptografia de chaves públicas definidos pela RSA. Também são descritas as funcionalidades de cada padrão de acordo com a RSA [LAB]

Padrão	Definição
PKCS #1	Define padrões para criptografia de chaves pública usando o algoritmo RSA
PKCS #2	Incluído dentro do PKCS #1
PKCS #3	Especifica um padrão para o estabelecimento de uma conexão segura usando o algoritmo Diffie-Hellman
PKCS #4	Incluído dentro do PKCS #1
PKCS #5	Define recomendações para a implementação de algoritmos baseados em senhas
PKCS #6	Estabelece um padrão de sintaxe para certificados estendidos
PKCS #7	Descreve a sintaxe para dados assinados ou cifrados
PKCS #8	Estabelece um padrão para informações de chaves privadas
PKCS #9	Define tipos de atributos a serem usados nos padrões PKCS #6, PKCS #7, PKCS #8 e PKCS #10
PKCS #10	Descreve a sintaxe para requisições de assinaturas de certificados de chaves públicas
PKCS #11	Define uma API para dispositivos de armazenamento de informações de criptografia e funções de performance de criptografia
PKCS #12	Descreve um formato para o armazenamento e transporte de chaves privadas, certificados, etc..
PKCS #13	Especifica padrões para criptografia usando curvas elípticas.
PKCS #14	Define padrão para geração de números pseudoaleatórios
PKCS #15	Estabelece um padrão para assegurar que usuários poderão usar criptografia para autenticar-se em aplicações

A grande maioria das aplicações existentes utilizam esses padrões. Serão descritos dois desses padrões, os quais são utilizados largamente em infra-estruturas de chaves públicas.

2.8.1 PKCS #7

Padrão utilizado para a transferência de dados assinados ou cifrados. Ele também permite o encapsulamento de uma mensagem, assinada ou cifrada, dentro de uma nova mensagem, assim, uma mensagem pode ser cifrada e depois assinada[LAB 93].

O padrão é compatível com Privacy-Enhanced Mail (PEM), codificação utilizada na transferência de mensagens assinadas e cifradas por e-mail. Com essa compatibilidade, uma mensagem pode ser transferida através da Internet sem a necessidade de codificações adicionais.

Uma mensagem assinada consiste no cálculo da Função Resumo e sua cifragem por um ou mais indivíduos. O resultado deste processo é a assinatura digital do conteúdo da mensagem. Para cada indivíduo que assina a mensagem, uma Função Resumo é calculada utilizando o algoritmo especificado. Se o indivíduo quer autenticar um bloco de dados além do conteúdo, o Resumo da Mensagem é calculado sobre o conteúdo juntamente com as outras informações desejadas. O resultado disto será assinado utilizando a chave privada de cada indivíduo. Juntamente com a mensagem e sua assinatura é enviado o certificado digital do assinante, para que seja feita a verificação.

Quando alguém deseja cifrar uma mensagem, antes do processo de cifragem ser iniciado é gerada uma chave simétrica, denominada chave de cifragem, com o objetivo de tornar o processo mais rápido. Esta chave é enviada juntamente com a mensagem cifrada. Uma mensagem com o conteúdo cifrado e sua chave de cifragem é denominada mensagem envelopada. No envio da mensagem, a chave de cifragem é cifrada com a chave pública de cada indivíduo, que receberá a mensagem e o seu conteúdo cifrado utilizando a chave de cifragem. No recebimento da mensagem envelopada, o indivíduo usa sua chave privada para decifrar a chave de cifragem, e a utiliza para decifrar o conteúdo da mensagem.

2.8.2 PKCS #10

PKCS #10 é o padrão para requisições de certificados. Uma requisição é formada pela identificação do requisitante e uma chave pública, juntamente com outros atributos opcionais. Todo o conjunto de dados é assinado digitalmente pela entidade que está requerendo a certificação. Requisições para certificados são enviadas para AC, que as transformam em certificados digitais. Após criado o certificado digital, a AC envia o certificado para a o requisitante.

A requisição é assinada para evitar que uma entidade execute a requisição de assinatura utilizando a chave pública de outra entidade. Esse procedimento impede que uma outra entidade personifique a AR gerando problemas de segurança. Esse padrão não é compatível com PEM[LAB 00].

2.9 Conclusão

Para a realização de uma transação é necessário que ambas as partes sejam identificadas e que as informações sensíveis sejam tratadas de forma confidencial. A criptografia e os serviços dela derivados tornaram possíveis a criação de protocolos para garantir a execução de transações em forma eletrônica. Através do uso da criptografia é possível identificar alguém através de sua assinatura digital e trocar mensagens de maneira confidencial.

Capítulo 3

Infra-estrutura de Chaves Públicas

3.1 Introdução

Este capítulo aborda os componentes necessários para o funcionamento de uma ICP. Além disto, o capítulo discorre sobre os vários modelos de ICP existentes, e diferencia políticas de certificação de declaração de práticas de certificação.

Uma ICP consiste em uma rede de protocolos, padrões e serviços, para suportar aplicações de criptografia de chaves públicas. A ICP define e estabelece a identidade de um usuário para autenticação e autorização[WRI 99].

No entanto, para viabilizar o uso de uma ICP é necessária a criação de uma estrutura que possibilite a correta operação da parte técnica. Esta estrutura é responsável, por exemplo, pela organização da área burocrática como o armazenamento dos documentos [FER 01].

A seção 3.2 faz uma introdução sobre certificados digitais. As seções 3.3 e 3.4 descrevem as funcionalidades de uma AC e de uma Autoridade de Registro respectivamente. A seção 3.5 caracteriza um diretório público. A seção 3.6 define o que são entidades finais. A seção 3.7 aborda as funcionalidades do módulo público. A seção 3.8 aborda os modelos de ICP existentes. A seção 3.9 demonstra o funcionamento de um caminho de certificação. As seções 3.10 e 3.11 fazem uma diferenciação entre políticas de certificação e declaração de práticas de certificação.

3.2 Certificados Digitais

Um certificado digital é uma estrutura que relaciona dados de uma pessoa ou máquina a uma chave pública [FER 01]. Certificados digitais permitem a autenticação de um sujeito ou dispositivo. Como os certificados digitais possuem a chave pública da entidade, ele pode ser usado para cifrar dados, garantindo assim, a confidencialidade.

Certificados digitais possuem um tempo de vida formado pela data de início da validade do certificado e a data que o certificado deixará de ser válido. Um certificado necessita ter um prazo de validade devido à evolução dos dispositivos de processamento. O certificado possui uma chave pública com um tamanho definido, determinado pelo número de bits. Com o passar do tempo, o tamanho da chave contida no certificado pode ser considerado fraco, ficando sujeita a ser quebrada por computadores com alto poder de processamento [NOT 02].

Como o certificado possui um tempo de validade, quando ele for renovado, o ideal é gerar um novo par de chaves com tamanho maior que o anterior. Isto evitaria que após um tempo o certificado possua um par de chaves considerado fraco.

Também é possível determinar o fim da validade de um certificado digital antes da sua data de expiração, isso é feito através da sua revogação. Um certificado digital pode ser revogado por uma série de fatores que serão explicados no capítulo 4.

Um certificado digital é formado, basicamente, pelos seguintes campos: versão do certificado, número serial, algoritmo de assinatura, dados do emissor, validade, dados do sujeito, informações da chave pública, identificador do emissor, identificador do sujeito. Estes campos serão explicados com detalhes no capítulo 4. A figura 3.1 mostra a estrutura de um certificado digital.

3.3 Autoridade Certificadora

Autoridade Certificadora (AC) é a entidade responsável pela assinatura e emissão de certificados digitais. A AC também pode ser responsável pela revogação de certificados digitais.

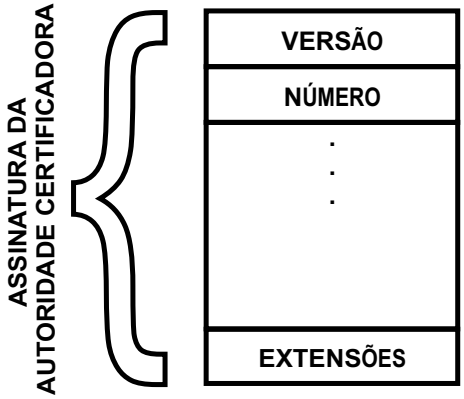

Figura 3.1: Um certificado digital é formado por um conjunto de campos padrões como, por exemplo, número da versão, número único de identificação do certificado, etc.. Além destes campos, um certificado também possui campos de extensão, eles são necessários para definir as funções do certificado, personalizar um certificado, etc..

Uma AC recebe uma solicitação para assinatura e a processa de acordo com um conjunto de regras. O resultado do processamento é a emissão do certificado correspondente à requisição.

A AC deve ser uma entidade confiada pelo solicitante do certificado e pelos outros indivíduos que ele deseja estabelecer uma comunicação. A AC é responsável por garantir a identidade das entidades durante uma comunicação.

3.4 Autoridade de Registro

Uma Autoridade de Registro (AR) provê uma interface entre um usuário e uma AC. Ela é responsável por conferir as informações do usuário e envia a requisição do certificado para a AC. A qualidade do processo de conferência das informações determina o nível de confiança que deve ser atribuído ao certificado [HUN 00].

A AC deve, obrigatoriamente, confiar na AR, pois a AC irá assinar as informações enviadas pela AR sem nenhuma verificação adicional. A confiança é necessária para garantir o funcionamento de todas as etapas do processo.

Dependendo do volume de certificados emitidos pela AC, pode ser definido um conjunto de AR. Estas AR são denominadas, normalmente, Autoridades de

Registro Locais (ARL). Outro motivo para a criação de ARL é devido à emissão de certificados de diferentes tipos. Como o próprio nome já define, as ARL são distribuídas geograficamente, balanceando o número de requisições recebidas individualmente.

3.5 Diretório Público

Ao contrário da chave privada, o certificado digital pode, e em alguns casos deve ser distribuído sem qualquer restrição. A distribuição dos certificados é, normalmente, efetuada através da publicação dos certificados em diretórios públicos. Além de certificados de usuários finais, o diretório público pode armazenar também certificados de AC e listas de certificados revogados (explicadas na seção 4.5).

O diretório público não necessita estabelecer uma conexão segura com o usuário no momento da busca e download de um certificado. O certificado é conferido através de sua assinatura digital. O diretório público deve, somente, possuir os dados atualizados, além de assegurar ao usuário bons mecanismos para manter seu nível de disponibilidade muito alto.

A obtenção do certificado digital de um indivíduo é necessária quando deseja-se uma troca de informações confiável. Isto é preciso porque as informações são cifradas com a chave pública contida no certificado.

Os diretórios, em sua grande maioria, são baseados nos serviço de diretório X.500 e LDAP.

3.5.1 Serviço de Diretório X.500

O X.500 foi um dos primeiros modelos de serviços de diretórios. Ele define um protocolo de acesso ao diretório e o modelo de informação que define como dados são armazenados e gerenciados[AUS 01].

O padrão X.500 foi criado pela ISO em 1988, e desde então tem sofrido uma série de revisões que incluíram suporte para controle de acesso e programa de gerenciamento. O X.500 permite a usuários e aplicações acessar diretórios sem a consciência

que os servidores de diretórios estão distribuídos.

Um dos motivos pelo qual o protocolo X.500 não tornou-se um padrão na Internet foi o seu desenvolvimento voltado para trabalhar com o protocolo OSI, que não é portável na internet.

3.5.2 LDAP

Para suprir a necessidade na Internet de acesso a diretórios foi criado o *Lightweight Directory Access Protocol* (LDAP). O LDAP pode ser visualizado como um banco de dados distribuído, no qual cada registro incluído é organizado dentro de hierarquia de nomes. Os registros são acessados através do uso de funções semelhantes às utilizadas em banco de dados [Jag 99].

O LDAP foi desenvolvido para ser um protocolo leve e flexível e, diferentemente do X.500 que trabalha somente com o protocolo OSI, ele trabalha com o protocolo TCP/IP. Como o LDAP foi otimizado para trabalhar com o protocolo TCP/IP ele, rapidamente, tornou-se um padrão para acesso de diretórios na Internet.

O resultado disso é que os servidores de diretórios oferecidos por diferentes fornecedores, apresentam cada um, um tipo de solução diferente para acessar as funções internas de diretório. Organizações que trabalham com múltiplos servidores de diretórios podem encontrar problemas de compatibilidade.

3.6 Entidades Finais

Uma Entidade Final é qualquer objeto que utilize um certificado digital, excluindo os próprios componentes da ICP. Este objeto pode ser um sujeito, uma aplicação, um dispositivo, etc..

A Entidade Final faz uma solicitação de um certificado digital, aguarda todo o processo para a sua emissão e, finalmente, o utiliza para os fins específicos.

3.7 Módulo Público

O Módulo Público fornece uma interface para que a entidade final possa fazer a solicitação de um certificado. Como a entidade final não pode ter acesso a uma AR ou uma AC, todas as funcionalidades que podem ser utilizadas por ele devem estar disponíveis nesse módulo.

No Módulo Público encontra-se também listas de certificados revogados e certificados digitais de AC. Isto garante ao usuário que todas suas necessidades serão supridas sem a necessidade de acesso a uma AC.

Uma única AC pode conter vários módulos públicos.

A figura 3.2 é a visão geral do funcionamento de uma ICP.

3.8 Modelos de Confiança

Uma Infra-estrutura de Chave Pública pode ser organizada de diferentes maneiras, dependendo de seus objetivos. Cada modelo possui uma denominação de acordo com a maneira que as AC são arranjadas. Cada modelo define em quem cada entidade deve ou não confiar.

3.8.1 Modelo Isolado

O Modelo Isolado é o mais utilizado atualmente. Ele é formado por uma AC no topo, alguns níveis de AC, denominadas AC intermediárias, e as entidades finais. O modelo isolado é ilustrado na figura 3.3.

A AC que fica localizada no topo é denominada AC-Raiz. Esta AC é auto-assinada, ou seja, seu certificado é assinado usando sua própria chave privada. Abaixo da AC-Raiz pode haver vários níveis de AC intermediárias. O número máximo de níveis abaixo é definido pela AC do nível atual.

No Modelo Isolado a confiança é centralizada na AC-Raiz, sendo transmitida para os usuários finais através das AC intermediárias. Neste modelo, é suposto que todos os usuários tenham conhecimento da AC-Raiz e de sua chave pública [Ada 00].

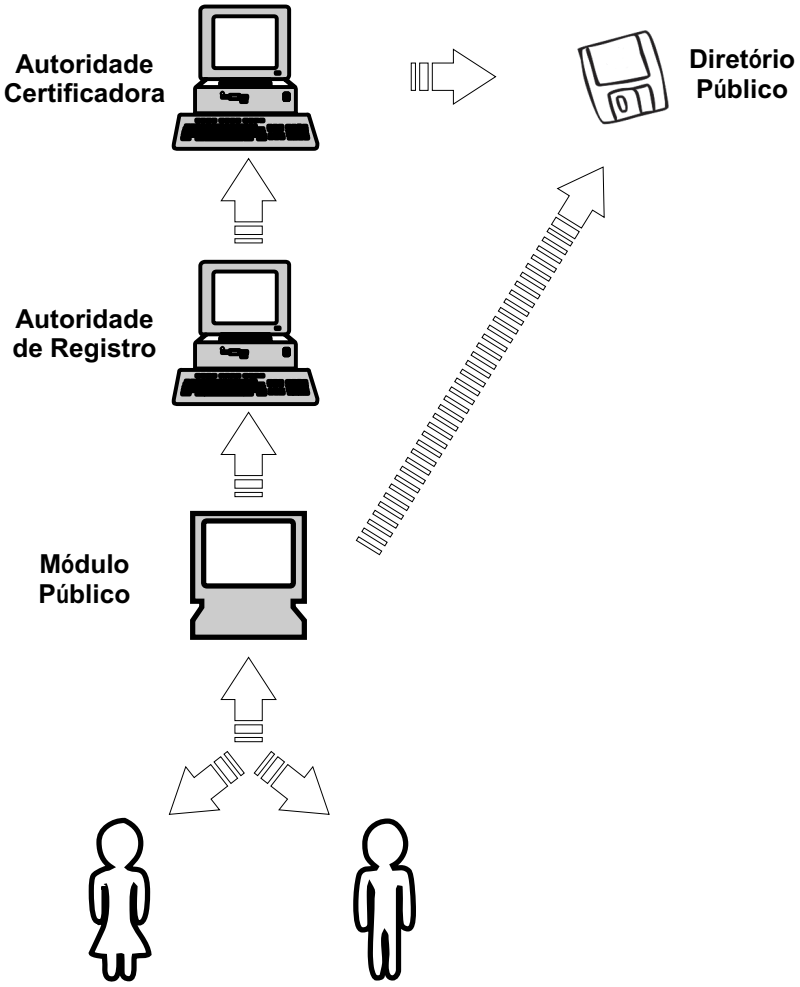

Figura 3.2: A requisição do certificado digital é feita pela entidade final usando o módulo público. Os dados da requisição são conferidos pela AR e se estiverem corretos são repassados para a AC. A AC emite o certificado digital e o envia para o diretório público. A entidade final usa o módulo público para acessar o diretório e recupera o certificado.

Uma AC-Raiz, normalmente, não deve emitir certificados para usuários finais. A emissão destes certificados é tarefa das AC intermediárias. Se a AC-Raiz permitir, elas também podem emitir certificados para outras AC abaixo delas.

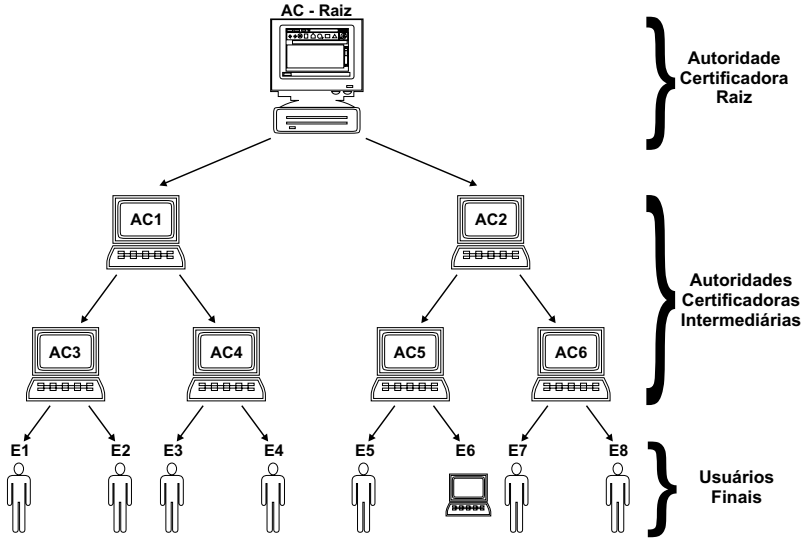

Figura 3.3: A hierarquia isolada possui apenas uma AC Raiz. Abaixo dela podem existir vários níveis de AC Intermediárias. Uma AC intermediária pode, ou emitir certificados para entidades finais, ou para outras AC abaixo dela.

3.8.2 Certificação Cruzada

Certificação cruzada é um mecanismo muito útil quando deseja-se estabelecer a confiança entre duas AC. Também é possível utilizar a certificação cruzada para diminuir/otimizar a descoberta do caminho de certificação.

Os dois tipos de certificação cruzada serão descritos abaixo:

Unilateral Neste tipo de certificação cruzada somente um dos certificados é assinado pela outra AC, ou seja, a AC_1 assina o certificado da AC_2, porém a AC_2 não assina o certificado da AC_1. Um exemplo deste tipo de certificação cruzada é ilustrado na figura 3.4.

Figura 3.4: Na certificação cruzada unilateral somente um dos lados possui confiança no outro. Na figura acima a AC2 confia na AC1. Esta confiança é atribuída pela assinatura do certificado AC2 pela AC1. Porém a AC1 não confia na AC2, pois esta não assinou seu certificado.

Mútua Envolve a assinatura dos certificados de ambas AC, ou seja, a AC_1 assina o certificado da AC_2, e esta assina o certificado da AC_1. Este tipo de certificação cruzada é ilustrado na figura 3.5.

Figura 3.5: Na certificação cruzada mútua, ambas as AC possuem confiança uma na outra. Na figura acima a AC2 confia na AC1 e vice-versa. Esta confiança é atribuída porque a AC2 assina a AC1 e a AC1 assina a AC2.

A certificação cruzada pode ser utilizada para garantir a confiança entre duas ICP não ligadas. Através da certificação cruzada poderia ser determinada a confiança para a validação de um certificado emitido por uma AC da ICP_1 em um sistema com certificado assinado por alguma AC da ICP_2.

3.8.3 Modelo em Floresta

Um Modelo em Floresta consiste de várias ICP distintas. Cada ICP pertencente a floresta pode seguir um modelo diferente das outras. As ICP integrantes da floresta podem possuir confiança entre si ou podem permanecer de forma isolada.

Caso as ICP estejam conectadas, o mecanismo de certificação cruzada é usado para estabelecer a confiança entre a AC-Raiz de um modelo com a AC-Raiz de

outro. Somente AC-Raízes devem utilizar certificação cruzada neste caso. Um exemplo de Modelo em Floresta é demonstrado na figura 3.6.

Atualmente, existem muitas ICP organizadas de diferentes modos. Não é possível, e também não será no futuro, criar uma floresta única. Isto é determinado por motivos políticos, geográficos e culturais.

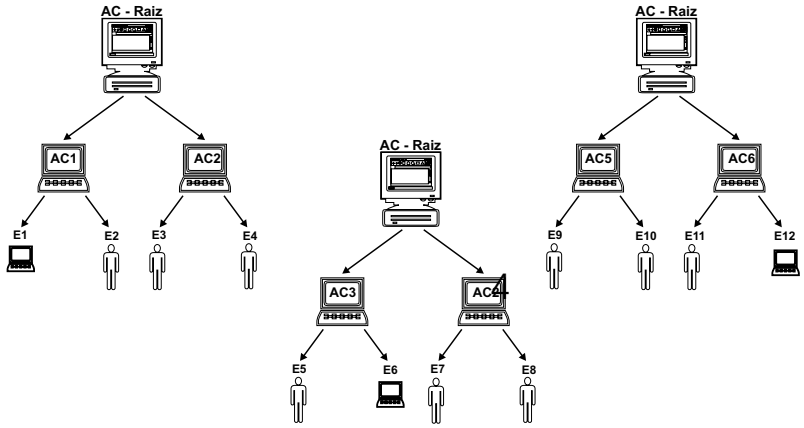

Figura 3.6: O Modelo em Floresta pode possuir várias AC Raiz. Estas autoridades podem ser conectadas através de certificações cruzadas. Cada ICP pode possuir vários níveis de Autoridades Certificadoras intermediárias. Cada AC intermediária pode emitir certificados para entidades finais ou para outras AC abaixo dela.

3.8.3.1 Modelo em Malha

No modelo em malha, a AC-Raiz de cada ICP possui uma certificação cruzada com as AC-Raízes de todas as outras ICP da floresta.

O modelo organizado em malha requer $(N^2 - N)/2$ certificações cruzadas, onde N é o número de ICP total da floresta. Isso não é obstáculo em ICP que não possuem uma grande quantidade de AC. Porém, à medida que o número de AC aumentam, o gerenciamento do sistema torna-se muito complexo.

Uma ICP organizada no modelo em malha é visto na figura 3.7.

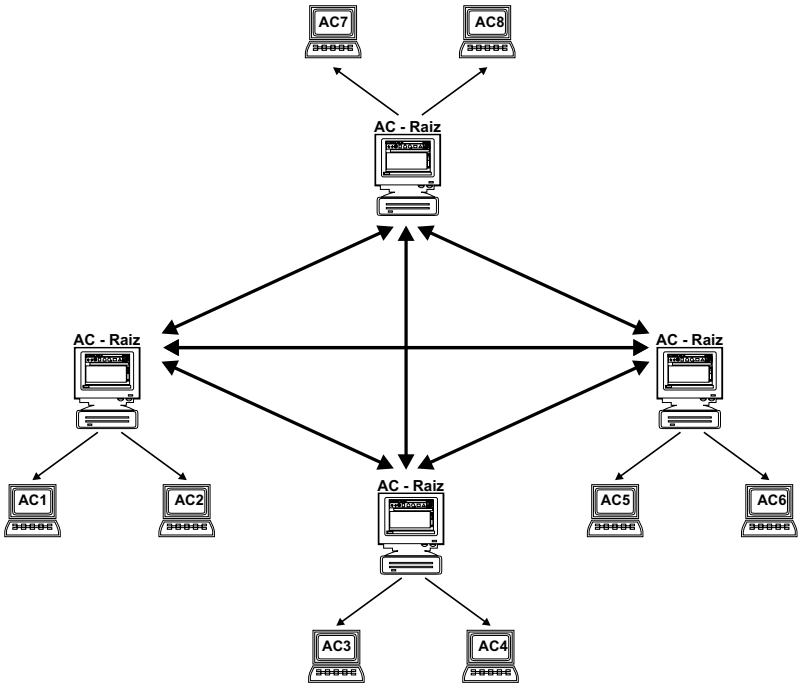

Figura 3.7: No Modelo em Malha cada ICP necessita fazer uma certificação cruzada com todas as outras ICP da floresta.

3.8.3.2 Modelo com Ponto Central

Neste tipo de modelo, cada ICP da floresta possui uma certificação cruzada com uma entidade central, denominada Ponte. Ou seja, a Ponte é o ponto de ligação entre todas as ICP da floresta. Uma estrutura utilizando uma Ponte é ilustrada na figura 3.8.

Em ICP que possuem uma grande quantidade de AC é aconselhável esse tipo de modelo, pois o gerenciamento é muito mais simples do que o Modelo em Malha. O gerenciamento torna-se mais simples neste modelo, devido ao menor número de certificações cruzadas que necessitam ser estabelecidas. Por exemplo, uma floresta com 10 ICP necessita apenas 10 certificações cruzadas com a entidade central, enquanto que no Modelo em Malha necessita de 45 certificações cruzadas.

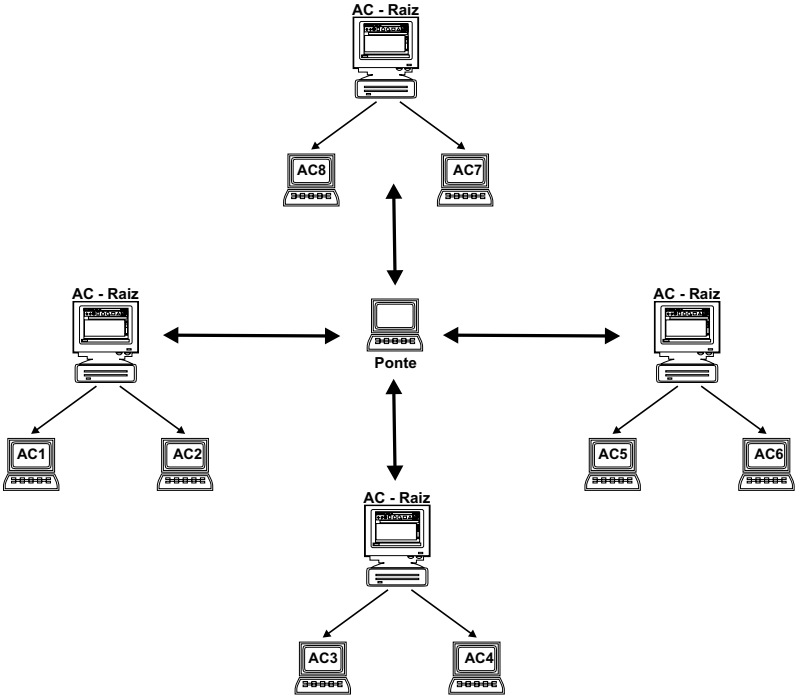

Figura 3.8: No modelo com ponto central é necessário apenas uma certificação cruzada de cada ICP com um ponto central.

3.8.4 Modelo Internet

Como na Internet existem muitas ICP localizadas em lugares ao redor do mundo, utilizando diferentes modelos, os navegadores criaram um novo modelo para poder atender a necessidade dos usuários das mais diversas ICP.

O navegador já traz instalado os certificados das AC-Raízes de algumas ICP, consideradas, por ele, confiáveis. Desta forma, as entidades finais que tiverem seus certificados emitidos por estas ICP serão, automaticamente, confiadas pelo navegador.

Quando é estabelecida uma conexão com uma entidade que foi assinada por uma AC de um nível inferior a alguma das AC-Raízes presentes no navegador, ou pela própria AC-Raiz, o navegador assumirá aquela entidade como confiável e estabelecerá a conexão normalmente. Se a entidade não for assinada por uma AC de nível inferior a algumas dessas AC-Raízes, o usuário deverá instalar o certificado da AC emissora do certificado antes de estabelecer a conexão. Caso não seja instalado, o navegador exibirá

mensagens alertando o usuário que a entidade não é confiada por ele.

3.9 Caminhos de Certificação

O caminho de certificação é formado por todos os certificados, iniciando pelo certificado da entidade final, passando por todas as AC intermediárias, até a AC-Raiz.

O caminho de certificação é necessário para determinar a confiança, ou não, em um certificado. No momento do recebimento de um certificado, cabe ao sistema descobrir se ele é, ou não, confiável. Isto é feito através do processamento do caminho de certificação.

Antes do sistema interpretar o certificado recebido como um certificado válido, ele monta todo o caminho de certificação e descobre se este possui algum certificado considerado ”confiável” por ele. Além disso, o sistema, também, procurará uma brecha no caminho de certificação, ou seja, algum certificado que possua restrições ou não pode mais ser considerado válido.

Se a AC emissora do certificado não for confiada pelo sistema e nenhuma outra AC do caminho de certificação possuir esta confiança, o certificado será assumido como não confiável pelo sistema e a conexão só continuará se o usuário assumir a responsabilidade da confiança [HOU 99].

O processamento do caminho de certificação é executado em duas etapas.

3.9.1 Determinação

A primeira fase é a determinação do caminho de certificação do certificado. Para isto, todos os certificados entre o sujeito e a AC confiável são buscados nos diretórios.

A busca dos certificados é efetuada começando pelo certificado da entidade final e seguindo em direção a AC-Raiz. Para isto é utilizado um campo de extensão do certificado digital que aponta para o certificado da AC superior.

A determinação também é responsável pela obtenção de todas as LCR (explicadas na seção 4.5) necessárias para validação, incluindo a verificação de sua integridade e validade.

3.9.2 Validação

Após determinado o caminho de certificação entre a entidade final e a autoridade no nível mais alto da hierarquia, há a necessidade de checar se não existe nada errado.

Ao contrário da determinação, a validação é iniciada na AC confiável e ”desce” até a entidade final.

De acordo com a RFC 2459, o objetivo da validação é estabelecer a ligação entre o nome distinto ou o nome alternativo do sujeito e sua chave pública, de acordo com a chave pública de uma AC de ”maior” confiança. Esta AC pode ser a AC-Raiz, a AC que emitiu o certificado que está sendo verificado, ou qualquer outra AC integrante da ICP.

Para a validação, as seguintes verificações são exercidas sobre cada certificado do caminho de certificação:

- Se a assinatura do certificado foi exercida por uma AC de nível imediatamente superior. No caso de uma AC-Raiz, a verificação da assinatura é feita com a chave pública do próprio certificado, ou este passo é omitido;
- Se o período de validade não expirou. A data e hora do computador do usuário são utilizadas para testar este passo;
- Se o certificado não está revogado, ou não está definido como suspenso em sua LCR. A data e hora do computador do usuário são utilizadas para testar esse passo;
- Se os dados presentes no campo sujeito do certificado são idênticos aos dados do campo emissor do certificado que o assinou;
- Verificar se não existe alguma(s) política(s) tornando o certificado inválido;

- Reconhecer e processar todas as extensões críticas presentes no certificado;
- Verificar a existência de alguns campos de extensão e, caso esteja presente, verificar se as suas características não invalidam o certificado.

Caso alguma das ações acima venha a falhar, o procedimento termina e o caminho de certificação é assumido inválido. Se todas as ações forem executadas com sucesso, o caminho de certificação é declarado válido.

3.10 Políticas de Certificação

Toda organização responsável por uma ICP deve elaborar um documento contendo suas políticas de certificação (PC), de forma a facilitar o entendimento do processo como um todo por seus usuários. Esse documento detalha todas as políticas instituídas pela organização para garantir a segurança do processo de emissão e manutenção dos certificados emitidos[MIG 02].

As PC descrevem o papel de cada componente dentro da ICP, as responsabilidades assumidas pelos seus usuários para a requisição e uso dos certificados digitais, além da manutenção do par de chaves. As políticas de certificação devem abranger desde a solicitação do certificado, até a sua expiração ou revogação.

As políticas de certificação não declaram os detalhes operacionais, pois estes podem ser alterados ao longo do tempo. Isso torna as PC um documento estável.

Se a ICP conter múltiplas AC, devem ser declaradas todas as AC que fazem parte das PC. Além disto, diferentes ICP poderiam utilizar as mesmas PC, caso possuam as mesmas políticas[HOU 01].

3.11 Declaração de Práticas de Certificação

Na Declaração de Práticas de Certificação (DPC) é especificado detalhadamente como cada componente de uma ICP implementa a política de certificação. A

DPC declara a PC associada e especifica os mecanismos e procedimentos utilizados para alcançar as políticas de segurança.

Uma DPC pode informar os aplicativos utilizados e os procedimentos de utilização do aplicativo. Ela deve estar suficientemente detalhada para comprovar que todas as políticas podem ser satisfeitas através de procedimentos e ferramentas[HOU 01].

Uma ICP deve declarar uma DPC para cada componente que a integra, porém, muitas vezes, podem haver dois componentes executando funções semelhantes. Neste caso, uma única DPC pode ser usada para ambos os componentes.

3.12 Conclusão

Embora a criptografia atenda aos requisitos básicos de segurança, ela, por si só, não fornece determinadas garantias de segurança para assegurar seu uso na Internet. Para que os serviços por ela oferecidos sejam adequados para o uso via rede, foi criada uma estrutura formada por uma série de componentes distintos. Esta estrutura é determinada Infra-estrutura de Chaves Públicas.

A Infra-estrutura de Chaves Públicas permite-nos utilizar, com garantias de segurança, os serviços fornecidos pela criptografia.

Capítulo 4

Recomendação X.509

4.1 Introdução

Este capítulo descreve com detalhes o formato de um certificado digital de chave pública de acordo com a recomendação X.509, de certificados de atributos e, também, das listas de certificados revogados.

O capítulo comenta os principais tipos de Listas de Certificados Revogados e seus mecanismos para disseminação.

A seção 4.2 descreve todos os detalhes de um certificado X.509. A seção 4.3 caracteriza um certificado de atributo. A seção 4.4 aborda maneiras de estabelecer restrições do uso de determinados certificados digitais. Finalmente, a seção 4.5 descreve uma lista de certificados revogados, seus formatos e métodos de disseminação.

4.2 Certificado Digital

Um certificado digital é uma associação entre uma chave pública e uma entidade. Esta entidade pode ser uma pessoa ou um dispositivo [FEG 99]. Todo certificado possui uma chave privada relacionada com a chave pública incluída nele.

Embora existam vários tipos de certificados em uso na Internet, a maior aceitação é pela recomendação X.509 do ITU-T.

O primeiro trabalho realizado envolvendo ICP e o uso de certificados digitais resultou, em 1988, na definição da primeira versão da recomendação X.509 v1. Ela foi parte da primeira edição da recomendação do serviço de diretório X.500 (referenciado na seção 3.5) [MIT 00].

O certificado X.509 v1 possui um número pequeno de campos e isto limita sua utilização. Além disto, foram encontrados problemas de segurança na recomendação. A figura 4.1 descreve um certificado X.509v1.

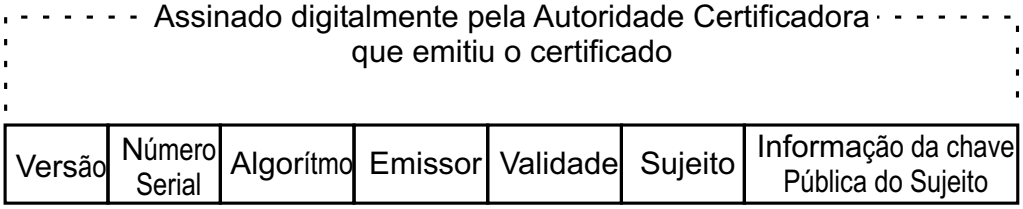

Figura 4.1: Estrutura de um certificado digital X.509v1.

Devido aos problemas de segurança, a primeira versão foi totalmente revisada e, em 1993, foi emitida a segunda versão. Nesta versão foram incluídos novos campos com o objetivo de possibilitar a reutilização de nomes iguais em diferentes certificados digitais. Porém estes campos raramente são utilizados na atualidade. A figura 4.2 mostra um certificado digital X.509v2 [STA 99].

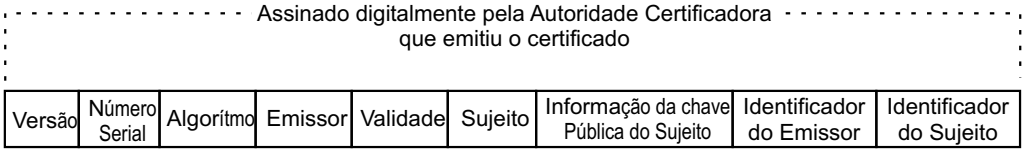

Figura 4.2: Estrutura de um certificado digital X.509v2.

A recomendação encontra-se, atualmente, na terceira versão. O ITU-T emitiu esta versão em junho de 1997. Nela foram adicionados campos de extensão, o que torna possível uma personalização maior do certificado. A inclusão de extensões tornou o uso de certificados digitais mais abrangente. A estrutura de um certificado X.509v3 é ilustrado na figura 4.3.

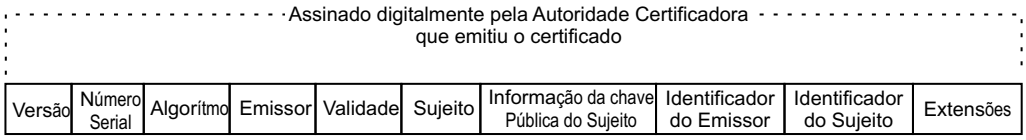

Figura 4.3: Um certificado digital é uma estrutura de dados dividida em três partes. Um conjunto de campos padrões que seguem a recomendação X.509v3. As extensões que são campos que podem variar de acordo com o tipo do certificado. Também podem ser incluídas extensões privadas. A assinatura do certificado é efetuada pela AC que o emitiu.

Um certificado digital é formado por um conjunto de campos definidos pela recomendação X.509v3, os quais serão listados abaixo:

Versão Identifica a versão do certificado. A versão pode ser 1, 2 ou 3;

Número Serial Identificador único de um certificado em relação a AC que emitiu-o;

Identificador do Algoritmo de Assinatura Campo que identifica o algoritmo usado pela AC para assinar o certificado;

Nome do Emissor Informações que identificam a AC emissora do certificado;

Período de Validade Intervalo de tempo que um certificado pode ser considerado válido. Este campo possui a data que o certificado foi emitido pela AC e a data de expiração do certificado;

Sujeito Dados de identificação do indivíduo ou dispositivo ao qual o certificado foi emitido;

Informações sobre a Chave Pública do Sujeito A chave pública do certificado, juntamente com identificador do algoritmo que a chave pública deve utilizar em suas operações;

Identificador do Emissor Valor único para a identificação do emissor do certificado;

Identificador do Sujeito Valor usado para a identificação do possuidor do certificado;

Extensões A Versão 3 da recomendação X.509 definiu utilização de campos de extensões com a finalidade de tornar mais flexível a utilização dos certificados digitais. Estes campos serão abordados em seguida.

Um certificado digital é sempre assinado por uma AC. Esta entidade deve possuir a confiança do indivíduo que utilizará o certificado, pois é ela que assegura a validade dos dados contidos no certificado digital.

4.2.1 Extensões

A versão 3 da recomendação X.509 definiu um conjunto de campos extras e a possibilidade da atribuição de novos valores para um certificado. Estes campos são denominados campos de extensão. Os campos de extensão podem ser divididos em dois tipos: críticos e não-críticos. Os campos de extensão considerados críticos são definidos pela recomendação do ITU-T.

Um campo de extensão é formado por três partes: o tipo da extensão, o indicador de criticidade e o valor da extensão. O tipo da extensão é formado por um código que identifica a extensão e seu tipo de dados. O indicador de criticidade define se a extensão definida pode ser ou não ignorada. Uma aplicação pode ignorar uma extensão não-crítica, caso ele não a reconheça. Porém, a aplicação deve rejeitar um certificado que possua uma extensão crítica que não seja reconhecida por ela. O campo valor da extensão possui o valor da extensão, este deve estar de acordo com o definido no tipo da extensão[FEG 99].

4.2.1.1 Extensões Definidas pela Recomendação X.509v3

As seguintes extensões são definidas pela recomendação X.509[UNI 97]:

Uso da Chave Indica o(s) propósito(s) para o qual a chave pública do certificado pode ser utilizada. Esta extensão pode ser crítica ou não-crítica;

Uso Estendido da Chave Indica o propósito para o qual a chave pública do certificado pode ser utilizada, em adição ou substituição ao propósito definidos no campo ”Uso

da Chave". Este campo pode ser crítico ou não-crítico;

Políticas de Certificado Lista as políticas válidas para o certificado. Elas devem ser reconhecidas pela AC emissora. Esta extensão pode ser crítica ou não-crítica;

Identificador da Chave da Autoridade Identifica a chave pública que deve ser utilizada na verificação da assinatura do certificado. Esta extensão deve ser não-crítica;

Identificador da Chave do Sujeito Este campo é uma "impressão digital" da chave pública do certificado. Esta extensão deve ser não-crítica;

Ponto de Distribuição da LCR Aponta para o local, ou locais, onde a LCR correspondente ao certificado está armazenada. A aplicação cliente encontrará a LCR atualizada, para conferir se o certificado em processamento está revogado. Esta extensão pode ser crítica ou não-crítica;

Período para Uso da Chave Privada Período de uso, contendo a data de início da validade e a data de expiração, da chave privada correspondente a chave pública do certificado. Este campo é aplicado somente em chaves para assinatura digital. Esta extensão deve ser não-crítica;

Mapeamento de Políticas Esta extensão deve ser usada somente em certificados emitidos para AC. Ela permite ao emissor do certificado indicar políticas de certificados que devem ser consideradas equivalentes em seu domínio. Estas políticas afetam todos os certificados de usuários que fazem parte do caminho de certificação da AC que definiu esta extensão. Esta extensão deve ser não-crítica;

Nome Alternativo do Sujeito Este campo contém um ou mais nomes alternativos para o sujeito do certificado. Esta extensão deve ser não-crítica;

Nome Alternativo do Emissor Este campo contém um ou mais nomes alternativos para o emissor do certificado. Esta extensão pode ser crítica ou não-crítica;

Atributos de Diretório Neste campo são atribuídos valores de Atributos de Diretório para o sujeito do certificado;

Impedimentos Básicos Indica se o sujeito do certificado pode agir como uma AC, utilizando a chave pública do certificado para verificar a assinatura digital de outros certificados. Esta extensão pode ser crítica ou não-crítica;

Impedimentos sobre Nomes Indica um espaço de nomes de sujeitos que deveriam ser localizados dentro do caminho de certificação. A busca deve começar a partir do certificado que declara o impedimento. A extensão deve ser utilizada somente em certificados de AC. Esta extensão pode ser crítica ou não-crítica;

Impedimentos sobre Políticas Especifica a obrigação de declarar explicitamente identificações de políticas de certificados ou inibir mapeamentos de políticas atribuídos. Este campo age sobre o restante do caminho de certificação. Esta extensão pode ser crítica ou não-crítica;

4.2.1.2 Extensões Particulares

A recomendação X.509v3 permite a criação de extensões particulares, ou seja, uma AC ou uma empresa pode inserir extensões cuja finalidade somente elas conheçam. A criação deste tipo de extensão facilita o desenvolvimento de aplicativos personalizados. Além disso, possibilita a inserção de dados que não podem ser inseridos nos campos e extensões definidas pela recomendação.

Um exemplo de uso de extensões particulares seria para liberar acesso a informações sensíveis em uma Intranet. Para isto basta a empresa definir a extensão ”privilegiada”. Após a definição, deve-se configurar o sistema para procurar por esta extensão e tratá-la. Se ela for encontrada, o sistema libera o acesso ao diretório onde estão localizadas as informações. Caso contrário, o sistema bloqueará o acesso.

4.3 Certificados de Atributos

Certificado de Atributo é uma estrutura de dados à parte de um certificado de chave pública. Porém, as informações contidas em um certificado de atributo estão associadas com um sujeito de um certificado de chave pública.

O sujeito de um certificado de chave pública pode possuir vários certificados de atributos associados a ele. Cada um destes certificados de atributos carrega certas propriedades referentes ao sujeito do certificado de chave pública. A AC que emitiu o certificado de chave pública não é obrigada a emitir também o certificado de atributos, pois este possui um campo identificando a AC que o emitiu.

Assim como certificados digitais, certificados de atributos podem ser revogados. Se um certificado de atributo é revogado, o respectivo certificado de chave pública do sujeito continua válido.

Um certificado de atributo possui os seguintes campos:

Versão Identifica as possíveis versões para um certificado. A versão atual é 1;

Sujeito Este campo associa o certificado de atributo com o certificado de chave pública. Para isto ele pode conduzir ou o Número Serial ou o Nome do Sujeito do respectivo certificado digital;

Emissor Estabelece o nome da entidade que emitiu o certificado de atributo;

Número Serial Número único com a finalidade de identificar o certificado;

Assinatura Identifica o algoritmo de assinatura utilizado para assinar o certificado;

Atributos Estrutura que pode conter um ou mais atributos associados com o sujeito do certificado. Para cada atributo é atribuído um nome e o valor.

Identificador Único do Emissor Número único que identifica o emissor do certificado de atributo, caso o nome do emissor não seja suficiente para identificação;

Um certificado de atributo pode ser utilizado para determinar níveis de autenticação de usuários. Com ele, é possível definir níveis de permissões de um usuário em cada módulo de um sistema.

Os certificados de atributo permitem a inserção de extensões para a inclusão de dados não definidos pela recomendação X.509.

4.4 Restrições de Caminhos de Certificação

Uma AC pode especificar o número máximo de níveis que podem existir abaixo da mesma. Isto é feito definindo valores para certas extensões de seu certificado.

4.4.1 Restrição por Níveis

Como foi visto anteriormente, existe uma extensão que define se o certificado é relativo a uma AC ou a uma entidade final, esta extensão é denominada **Impedimentos Básicos**. Se esta extensão for definida como crítica e o valor de um certificado de AC for definido, o certificado poderá ser utilizado para verificar assinaturas digitais de outros certificados. Além disto, surge a possibilidade de atribuir um valor para um segundo campo desta extensão, denominado **Impedimentos do Tamanho do Caminho**.

Este campo recebe um valor inteiro que é o número máximo de certificados de AC permitidos no caminho de certificação. A contagem é iniciada a partir do certificado ao qual o valor foi atribuído. Se for especificado o valor 0(zero), a AC poderá, somente, emitir certificados para entidades finais. Se nenhum valor for definido para o campo em nenhum do certificados do caminho de certificação, a quantidade de níveis para o caminho de certificação não é definido, ou seja, não há restrição quanto ao número máximo de AC.

Se a extensão não estiver presente ou, estiver marcada como não crítica e não for reconhecida pela aplicação, ela deveria buscar outros modos para concluir se o certificado deveria, ou não, ser utilizado para verificar as assinaturas digitais de outros certificados.

4.4.2 Restrição por Nomes

As restrições através de nomes são feitas utilizando a extensão **Impedimentos sobre Nomes**. Se ela estiver presente, torna-se possível atribuir valores para duas estruturas, as quais são *permittedSubtrees* e *excludedSubtrees*. Para cada uma, é possível especificar o nome de uma ou mais subárvores. Este campo agirá sobre a AC que possua

o nome especificado e, opcionalmente, seus níveis subjacentes.

Se o campo *permittedSubtrees* estiver presente, de todos os certificados emitidos pela AC e por outras AC abaixo, somente serão aceitos certificados com o campo ”Nome do Sujeito” com o valor determinado na extensão.

Se o campo *excludedSubtrees* estiver presente, qualquer certificado emitido pela AC e pelas AC subseqüentes no caminho de certificação, que possuam o campo ”Nome do Sujeito” com o valor determinado na extensão será negado.

Se ambos os campos estão presentes e possuem nomes iguais, os valores definidos no campo *excludedSubtrees* terão precedência.

4.4.3 Restrição por Políticas

As restrições através de políticas são exercidas utilizando a extensão **Impedimentos sobre Políticas**. Esta extensão é formada por duas estruturas, denominadas *requireExplicitPolicy* e *inhibitPolicyMapping*.

Caso algum valor seja atribuído ao componente *requireExplicitPolicy*, todos os certificados do caminho de certificação abaixo da AC, devem ter na extensão Políticas do Certificado, um identificador de política aceitável. Ou seja, deve possuir o identificador de uma política requerida pelo componente *requireExplicitPolicy*, ou ainda, uma política declarada como equivalente através do campo Mapeamento de Políticas.

Se o componente *inhibitPolicyMapping* estiver presente, não é permitido mapeamento de políticas, desde a AC que possui a extensão até o final do caminho de certificação.

Ambos componentes possuem um valor determinado como *SkipCerts* que indica o número de certificados do caminho de certificação que deverão ser omitidos, antes de tornar o impedimento efetivo.

4.5 Listas de Certificados Revogados

As Listas de Certificados Revogados (LCR) podem ser definidas como uma estrutura de dados assinada por uma AC. Esta estrutura contém uma lista de certificados que não devem ser considerados válidos [ADA 99].

Embora um certificado digital possua uma data para sua expiração, algumas vezes é necessário que sua validade seja negada antes do término deste prazo. Com esta finalidade, um certificado pode ser revogado e, a partir deste momento, ele constará em uma lista contendo um conjunto de certificados inválidos.

Uma revogação pode ser efetuada por um dos seguintes motivos:

Comprometimento da Chave Privada do Certificado Indica que a chave privada do sujeito pode estar comprometida, tornando o certificado do sujeito não-confiável;

Comprometimento da Chave Privada da AC A chave privada da AC que emitiu o certificado pode estar comprometida, com isto não deve-se mais confiar nos certificados emitidos por ela;

Mudança de Filiação Alguma das informações do sujeito contidas no certificado foi alterada, com isto um novo certificado deve ser emitido;

Atualização Indica que o certificado foi atualizado;

Cancelamento da Operação O certificado não será mais utilizado para o propósito ao qual ele foi emitido;

Suspensão Temporária Indica que o certificado está, temporariamente, incluído na LCR. Atribuindo esta suspensão ao certificado, ele poderá ser retirado da LCR após um período de tempo ou definitivamente revogado;

Não Específico O certificado consta na LCR por algum motivo diferente dos apresentados acima.

As LCR também seguem a recomendação X.509 do ITU-T. Atualmente, encontra-se na versão 2. O formato de uma LCR é ilustrado na figura 4.4. Uma LCR é formada pelo seguinte conjunto de campos:

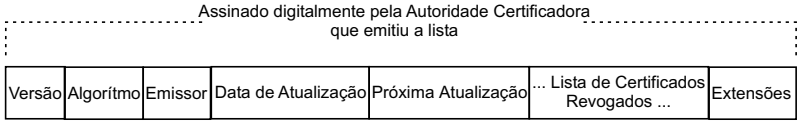

Figura 4.4: Uma lista de certificados revogados pode ser subdividida em três partes. Um conjunto de campos padrões que seguem o formato da recomendação X.509v3. Campos de extensões pré-estabelecidos pela recomendação e campos de extensões privados. A assinatura da lista de certificados revogados efetuada pela autoridade responsável pela emissão da LCR.

Versão Indica a versão da LCR. Esse campo é opcional e se não estiver presente, sua versão é 1. Isto porque o campo não havia sido definido na versão 1 da recomendação X.509;

Assinatura Identificação do algoritmo utilizado na assinatura digital da LCR;

Emissor Dados que identificam o emissor da LCR;

Atualização Data e hora de emissão da LCR;

Próxima Atualização Data e hora que uma nova atualização desta LCR deve ser emitida;

Certificados Revogados Lista contendo os números seriais de todos os certificados digitais revogados.

As LCR possuem dois tipos de extensões definidos. É definido um conjunto de campos de extensão para cada entrada de certificado revogado e um outro para a LCR como um todo.

4.5.1 Extensões por Entrada

Estas extensões são atribuídas para cada certificado revogado. Isto torna possível a inserção de informações extras para cada ítem individualmente. A recomendação

X.509v3 define as seguintes extensões para cada entrada da lista de certificados revogados:

Código da Razão da Revogação Identifica a razão pela qual o certificado foi revogado. Esse código pode ser usado por aplicações para definir como ela deverá tratar o certificado. Esta extensão é não-crítica;

Instruções de Suspensão Este campo permite a inclusão de uma instrução definindo uma ação a ser tomada em relação ao certificado suspenso. Esta extensão pode ser utilizada somente se no campo do Código da Razão da Revogação estiver especificado o valor como Suspensão Temporária. Esta extensão é não-crítica;

Data Inválida Indica a data a partir da qual o certificado é suspeito ou conhecido de ter sua chave privada comprometida, ou seja, que o certificado deveria ser considerado inválido. Esse campo pode possuir uma data anterior a data de revogação do certificado contido nessa entrada, e também, anterior a data de outras LCR já emitidas. Porém, somente esta extensão não é o suficiente para propósitos de irretratabilidade. Esta extensão é não-crítica;

Emissor do Certificado Identifica o emissor do certificado associado com uma entrada em uma LCR indireta(ver 4.5.4.5). Se esse campo não estiver presente na primeira entrada da LCR, o emissor do certificado é a mesma entidade que emitiu a LCR. Nas demais entradas, se ele não estiver presente, será considerado que o emissor é o mesmo da entrada anterior. Esta extensão é crítica.

4.5.2 Extensões por LCR

Número da Lista de Certificados Revogados Contém um número seqüencial identificando a LCR;

Ponto de Distribuição do Emissor Aponta para um local onde a LCR esteja armazenada, como um diretório público por exemplo. Esse campo indica se a LCR contém

apenas certificados de entidades finais, somente de AC ou somente certificado revogados por uma certa razão. Nesse campo também é atribuído um valor, caso a LCR contenha notificações de revogação de outras AC;

Identificador da Chave da Autoridade Identifica a chave pública que deve ser utilizada na verificação da assinatura da Lista de Certificados Revogados. Esta extensão é não-crítica;

Indicador de uma LCR Delta Indica que a LCR como sendo do tipo Delta (consultar 4.5.4.4). Esta extensão é sempre crítica;

Nome Alternativo do Emissor Um ou mais nomes alternativos associados com o emissor da LCR. Esta extensão pode ser crítica ou não-crítica.

4.5.3 Disseminação das LCR

As LCR devem ser disseminadas para que os usuários possam efetuar uma verificação do estado de um certificado desejado. Esta disseminação deve ser feita de maneira eficiente para que não ocorra problemas envolvendo a validação de certificados já revogados pela AC.

O tempo e o método de disseminação é definido de acordo com o tipo de uso do certificado. Uma LCR de certificados emitidos, onde em sua política de uso está definido que ele será utilizado para transações de baixo custo, é publicado utilizando intervalos de tempo maiores que uma LCR para certificados utilizados em grandes transações bancárias.

As listas de certificados revogados devem ser armazenadas em lugares que garantam sua disponibilidade, para que possam ser armazenadas em diferentes momentos. Elas não necessitam utilizar canais seguros para sua conferência. Sua segurança é garantida através da assinatura digital da AC.

4.5.3.1 Consultas Periódicas

Este método armazena as LCR em um diretório público ou em um sítio. A aplicação cliente tem a necessidade de executar consultas periódicas ao local e buscar a LCR mais recente.

Para garantir o sucesso deste método, é necessário que a aplicação acesse o site a cada nova atualização da LCR.

Pode ocorrer problemas com este método, caso não seja possível a aplicação acessar a LCR por um período. Isto pode ocasionar na confiança em um certificado já revogado.

4.5.3.2 Método Empurrar

Este método possui uma entidade, como a AC emitente, que envia a LCR cada vez que um novo certificado é revogado. Isto garante uma demora muito pequena entre a atualização da LCR e a atualização da aplicação cliente.

Porém, podem ocorrer problemas com a aplicação cliente caso o protocolo não defina um modo de garantir que a LCR foi, com certeza, recebida por todos os clientes aos quais ela foi enviada. Um outro problema poderia ser visto no caso da LCR ser distribuída para uma grande quantidade de aplicações, em pequenos períodos de tempos. Isto poderia causar o congestionamento da rede da entidade encarregada de enviar a LCR.

4.5.3.3 Verificação On-line da LCR

A utilização de protocolos garante a verificação das LCR em tempo real, ou seja, no momento que é recebida uma mensagem assinada. Assim como o Método Empurrar ele garante a verificação da última versão da LCR, porém como nem todas verificações serão feitas simultaneamente, a probabilidade de congestionamento da rede onde a LCR está armazenada é menos provável.

Um exemplo é um protocolo denominado Protocolo de Estado de Certificados On-line (OCSP). Ele foi projetado para verificar a validade dos certificados X.509,

mas pode trabalhar com outros tipos de certificados. Para determinar a validade, o protocolo usa campos de extensões do certificado X.509 [Woh 00].

Para garantir a exatidão na consulta aos certificados revogados, todas as mensagens trocadas pelo protocolo são assinadas. Isto garante a integridade e autenticação das consultas.

4.5.4 Disponibilização das LCR

Além das maneiras que uma LCR pode ser disseminada para uma aplicação, também existem vários modos de formatação para uma LCR, visando agilizar sua consulta. Cada modo de formatação pode ser associado a uma forma de disseminação distinta.

A melhor associação entre a formatação e a disseminação da LCR está relacionada com o tipo de aplicação para a qual ela será utilizada.

4.5.4.1 LCR Completa

Uma única LCR contém toda a informação dos certificados revogados pela AC. Este método pode ser utilizado em AC que não possuam um grande número de certificados emitidos. Caso contrário, isto não seria possível, pois o crescimento da LCR tornaria sua descarga uma tarefa pouco prática.

Esta situação pode ser aplicada em uma AC corporativa, pois este tipo de AC possui um número pré-determinado de certificados emitidos. Além disto os certificados serão, em sua maioria, emitidos e utilizados somente dentro da organização. Com isto todas as operações, como a busca da LCR, seriam feitas utilizando uma rede local. Este tipo de rede possui grande estabilidade e velocidade.

4.5.4.2 Listas de Autoridades Revogadas

Uma Lista de Autoridades Revogadas (LAR) possui a mesma estrutura de uma LCR, porém ela só possui informações sobre AC que tiveram seu certificado revogado. Em uma LAR não existem entradas de certificados de usuários finais.

4.5.4.3 LCR Particionada

A LCR particionada evita a necessidade do sistema buscar uma LCR completa a cada nova atualização. Ela ainda permite que um mesmo fragmento da LCR seja disponibilizado em vários locais diferentes, impedindo assim o excesso de tráfego em uma única rede. Além disto, a AC possui uma garantia do aumento da disponibilidade da LCR, deixando a LCR disponível para uma grande quantidade de serviços.

Este tipo de LCR usa a extensão Ponto de Distribuição da LCR para especificar o lugar onde o atual fragmento dela encontra-se. A aplicação deve buscar cada fragmento e armazená-lo na máquina local, para garantir que nenhum certificado já revogado seja aceito.

Um problema deste método é que a extensão definindo os locais onde estarão os fragmentos é inserida na hora da emissão, impedindo que novos locais sejam incluídos sem a emissão de um novo certificado.

4.5.4.4 LCR Delta

Este método é uma fusão do método de LCR Particionada e LCR Completa. Ele utiliza dois tipos de LCR distintas.

A primeira é denominada LCR Base, esta LCR é disponibilizada obedecendo um período definido de tempo. A LCR Base contém todos os certificados revogados pela AC emissora. Esta LCR pode ser muito grande e, por causa disto, sua emissão deve ser em períodos prolongados de tempo, por exemplo, mensalmente.

O outro tipo é definido como LCR Delta, ela é uma LCR incremental à LCR Base. Deste modo ela pode ser disponibilizada, por exemplo, cada vez que um novo certificado é revogado. A LCR Delta possui todos os certificados da LCR Delta anterior e mais os últimos certificados revogados, com isto, não corre-se o risco de ficar desatualizado na perda de uma LCR Delta.

Várias LCR Delta podem ser emitidas entre cada emissão de uma nova LCR Base. Cada vez que uma nova LCR Base é emitida, a LCR Delta é emitida a partir dos novos certificados revogados.

4.5.4.5 LCR Indireta

Uma LCR Indireta possibilita a fusão de LCR de várias AC diferentes em uma única lista. A recomendação X.509 v3 já disponibiliza a estrutura necessária para a implementação deste método. Deste modo é possível a identificação individual, associando cada entrada com uma AC distinta.

Este tipo de LCR pode ser muito útil para garantir que todas as LCR de um caminho de certificação estejam atualizadas no momento da validação. Impedindo que um erro seja cometido pelo esquecimento de atualização de apenas uma das LCR necessárias na validação.

LCR Indiretas também diminuem a dificuldade de atualização, pois todas as informações estão reunidas. Uma LCR Indireta também pode ser disponibilizada em vários pontos diferentes buscando assim uma maior disponibilidade e evitando que ocorra grande perda de largura de banda da rede onde a LCR está armazenada.

4.6 Conclusão

A utilização de certificados digitais garante os serviços essenciais para a execução de transações via Internet. Com eles é possível garantir a autenticação das duas partes durante o estabelecimento da conexão e, também, a troca de informações de modo sigiloso.

Além do comércio eletrônico, também é possível o uso de certificados para outros fins, como troca de mensagens e para autenticação em sistemas internos.

Capítulo 5

Utilização de uma Estrutura de Código Aberto

5.1 Introdução

O capítulo descreve as características dos aplicativos que possuem o código fonte aberto. O capítulo, também, apresenta o movimento do código fonte aberto, comenta as suas vantagens e faz um paralelo dos tipos de licenças de aplicativos em relação à segurança.

Como a dissertação propõe o uso de código fonte aberto, o bom entendimento desta estrutura é necessário para tirar proveito de suas características.

A seção 5.2 aborda a história do movimento do código fonte aberto. A seção 5.3 explica outros tipos de licenças e suas desvantagens de uso. As seções 5.4 e 5.5 definem as características e as vantagens dos aplicativos com o código fonte aberto. A seção 5.6 expõe a motivação para a criação de um projeto utilizando aplicativos com o código fonte aberto.

5.2 O movimento do Código Aberto

Em janeiro de 1984, um desenvolvedor chamado Richard Stallman decidiu deixar seu trabalho no Massachusetts Institute of Technology para trabalhar em um novo projeto. Este projeto foi denominado GNU e possuía uma filosofia que tornava-o diferente de todos os outros já conhecidos.

Seu criador acreditava que todos os usuários de computadores deveriam ser livres para modificar os softwares e, também para distribui-los [PEA 00]. Os programas são desenvolvidos sobre as regras instituídas por um novo tipo de licença nomeada *Copyleft*. Ao contrário do *Copyright*, essa licença assegura a distribuição dos programas sem custos para o usuário.

A partir da criação do GNU deu-se início a uma nova comunidade na Internet, a comunidade do código aberto. A comunidade cresceu e o número de aplicativos desenvolvidos por ela começaram a destacar-se cada vez mais no mercado. Isto chamou a atenção de algumas empresas que começaram a acreditar que os aplicativos de código aberto poderiam ter qualidades iguais ou melhores do que os produtos proprietários. Com isso, grandes companhias começaram a apoiar e, também, investir nesse tipo de aplicativo.

A adoção do sistema operacional Linux por grandes empresas alavancou ainda mais o crescimento dos aplicativos de código fonte aberto. Pois a grande maioria, senão a totalidade, dos aplicativos incluídos, ou portados, no sistema operacional seguem a mesma filosofia.

Com a utilização em massa das empresas e dos usuários doméstico comprovou-se o valor dos programas de código fonte aberto.

5.3 Tipos de Licenças

Atualmente existe um grande número de características que podem variar em um aplicativo de acordo com tipo de sua licença. Estas características variadas podem trazer vantagens ou desvantagens dependendo da área de atuação da empresa que

o adquiriu. O tipo de licença de um aplicativo pode trazer vantagens para empresas de determinado setor, mas pode causar problemas para uma empresa de outro.

Por causa dessa variação que uma licença pode causar em uma empresa, foi feito um estudo da influência de determinadas licenças em aplicativos da área de segurança, mostrando porque uma ICP deve utilizar aplicativos que possuam o código fonte aberto.

5.3.1 Programa Proprietário

Programas proprietários são aplicativos que possuem o código fonte sobre o domínio de uma única empresa ou por uma grupo delas. Normalmente, a empresa não libera visualização do código fonte para análise de seus usuários, exceto com o estabelecimento de acordos envolvendo altos valores. Seu uso, modificação ou redistribuição também devem ser autorizados ou licenciados pela empresa proprietária, quando permitido.

Geralmente, os aplicativos com o código fonte proprietário não são auditados por nenhuma empresa externa. Dessa maneira não é possível garantir que o aplicativo execute exatamente o que é declarado em sua documentação. Não pode ser admissível que o controle de um aplicativo de tal importância esteja sobre os cuidados de uma única pessoa, ou de um grupo reduzido.

Também em razão do pequeno número de pessoas que possuem acesso ao seu código fonte a capacidade do programa possuir falhas é muito grande. Muitas destas falhas podem ser descobertas por pessoas mal intencionadas antes do desenvolvedor, causando sérios danos as empresas que utilizam o aplicativo.

Como esse tipo de aplicativo possui um proprietário e ele possui o controle das alterações dos módulos do programa, caso uma entidade tenha a necessidade que um novo módulo seja incluído no programa, ou deseja a alteração de alguma característica existente, ela dependerá totalmente da empresa desenvolvedora. Além disso, caso a empresa concorde com a inclusão ou alteração do módulo, será necessário aguardar todas as etapas necessárias para a execução do procedimento estabelecido pela desenvolvedora.

Este tempo estabelecido pelas empresas desenvolvedoras, por mais breve que sejam, são demasiadamente longos para serem considerados aceitáveis na área da segurança

5.3.2 Freeware

Os aplicativos com este tipo de licença são distribuídos gratuitamente, sem restrições de utilização para seus usuários. Igualmente aos programas proprietários, o código fonte desses aplicativos estão em posse de uma ou várias empresas, não sendo permitido sua visualização ou alteração.

Este tipo de licença normalmente é usada por empresas ainda não conhecidas no mercado, elas procuram atingir um determinado número de pessoas através da disponibilização de seus aplicativos gratuitamente.

Estes aplicativos, em sua maioria, tem seu desenvolvimento descontinuado pelas empresas, ou porque elas não conseguiram conquistar usuários e não sobrevivem ao mercado, ou porque elas conseguiram se tornar conhecidas no seu nicho e a distribuição de programas gratuitamente não é mais de seu interesse.

5.3.3 Shareware

Estes programas possuem um período de tempo de utilização pré-determinado. O aplicativo pode ser usado gratuitamente dentro deste período de tempo. Quando o período expira, o usuário deve licenciar o aplicativo para continuar o seu uso. Esse tipo de aplicativo normalmente tem um custo menor que os aplicativos proprietários, porém as empresas desenvolvedoras não definem muitas responsabilidades para si, abstendo-se da culpa por certos problemas.

Os aplicativos com esse tipo de licença possuem os mesmos problemas já descritos nos programas proprietários.

5.4 Definição de Código Aberto

A principal confusão ocorrida no dias de hoje é a definição do termo ”aplicativo com código fonte aberto”. Isso começou no ano de 1998 quando a comunidade do código aberto resolveu mudar o nome do inglês *Free Software* para *Open Source Software*. A definição foi mudada porque muitos estavam confundindo o termo *free* que definia a liberdade que o usuário teria em relação ao código fonte, com grátis, ou seja, nenhum valor para utilizá-lo[PRO].

Os aplicativos com código fonte aberto podem ser taxados por uma empresa, caso ela entenda necessário, porém esta empresa deve disponibilizar o código fonte para os seus usuários juntamente com o aplicativo compilado, dessa maneira está garantida a liberdade de alterar o código do sistema.

Apesar de grande parte dos aplicativos com o código fonte aberto serem distribuídos gratuitamente por seus desenvolvedores, isto não é uma regra.

5.5 Vantagens do Código Aberto

O aplicativos de código aberto possuem muitas características não disponíveis nos outros tipos. Essas características garantem algumas vantagens para seus usuários.

5.5.1 Personalização

A licença dos aplicativos de código aberto permite a modificação de parte ou da totalidade do seu código fonte. Empresas podem utilizar este recurso para fazer melhorias no aplicativo, adequando-o a suas necessidades. Por exemplo, pode-se incluir funcionalidades extras que só determinadas empresas necessitam, tornando o aplicativo mais completo e não precisando adquirir outro para executar aquelas funções.

Também pode-se retirar certas partes do código caso elas não sejam utilizadas. Isso garante uma otimização no processamento e pode diminuir seu tempo de

execução. A personalização assegura uma melhor utilização dos sistemas e, também, um ganho de tempo na realização das tarefas cotidianas.

5.5.2 Agilidade na Correção de Falhas e Atualizações

Assim como os aplicativos com código fechado, os programas com código aberto estão sujeitos a falhas de programação. Porém, os aplicativos com código aberto são corrigidos de maneira mais rápida. Isto ocorre porque, normalmente, a empresa distribuidora do programa recebe a notificação do problema e, juntamente, o código fonte corrigido para que possa ser disponibilizado para outros usuário que obtiveram os mesmos erros.

Por outro lado, quando uma falha é detectada em um aplicativo de código fechado, este erro deve ser comunicado a empresa e, somente a partir deste momento começam a ser tomadas providências para a correção do código.

Outro ponto que torna mais rápida as atualizações nos aplicativos de código aberto é o número de programadores que estão trabalhando em um único aplicativo. Enquanto em aplicativos com código fechado somente os funcionários da empresa desenvolvedora conhecem o código fonte e possuem capacidade para alterá-lo. Os aplicativos com código aberto são conhecidos por várias comunidades ao redor do mundo e grande parte delas possuem pessoas capacitadas a alterar os fontes do aplicativo.

5.5.3 Custos de Licenças

Embora encontre-se na Internet uma grande quantidade de programas com o código aberto sendo distribuídos gratuitamente, não é determinado na licença nenhum obstáculo para sua cobrança por parte das empresas. Porém mesmo os programas que são cobrados possuem um valor muito inferior aos programas com código fonte proprietário. Com gastos menores no licenciamento de aplicativos, as empresas podem investir o dinheiro restante em seus funcionários ou em outras áreas que necessitem recursos adicionais.

5.5.4 Suporte Técnico

Enquanto que somente as empresas desenvolvedoras podem prestar suporte para os aplicativos de código fechado, suporte para aplicativos de código aberto pode ser oferecido por outras pessoas ou entidade, pois estes também possuem acesso ao código do sistema e podem resolver os problemas existentes.

Também encontram-se na Internet vários grupos de discussões debatendo sobre cada detalhe do código dos aplicativos. Com isto, muitas vezes nem é necessário recorrer ao suporte técnico da empresa, pois as respostas são encontradas na própria Internet.

Devido a grande afinidade dos programadores em relação aos aplicativos de código fonte aberto, encontra-se na Internet uma quantidade muito maior de materiais sobre estes aplicativos do que sobre aplicativos proprietários.

5.5.5 Auditoria do Código

O uso de aplicativos com o código fonte aberto torna mais fácil o processo de auditoria. A auditoria pode ser realizada por qualquer empresa, localizada em lugares distantes geograficamente, apenas transferindo o código fonte para os computadores da empresa e analisando-os.

Através da disponibilização do código fonte na Internet é possível a realização de auditorias por qualquer pessoa que deseje entender o funcionamento do sistema. Com um número maior de pessoas auditando o sistema, ele se tornará muito mais confiável que um aplicativo auditado apenas pelos seus desenvolvedores.

5.5.6 Transparência

É possível, somente, garantir a transparência de um aplicativo através da visualização e compreensão do seu código fonte. Não é possível garantir que um aplicativo execute o que o desenvolvedor assegura sem a visualização de seu código fonte.

Um programa com o código proprietário pode executar, em paralelo,

programas de tal forma que o usuário não consiga detectar. Através disso, um desenvolvedor mau intencionado, pode criar um aplicativo que faça a função que o usuário espera, mas além disto, o aplicativo pode executar um outro processo que faça algo danoso no computador do usuário.

5.5.7 Garantia da Continuidade do Desenvolvimento

Uma grande vantagem dos aplicativos com o código fonte aberto é a garantia de continuidade no desenvolvimento da aplicação. Isto não pode ser verificado em aplicativos proprietários. O que aconteceria se uma empresa proprietária de um aplicativo perdesse todos os seus dados, incluindo as cópias de segurança? Ou se a empresa declarasse falência? Como seria possível continuar a desenvolver algo que não se possui?

Este problema não é constatado nos aplicativos com o código fonte aberto. No caso de uma empresa perder todos os seus dados, todos os usuários dos aplicativos possuiriam uma cópia que poderia ser utilizada para continuar o desenvolvimento.

No caso do desenvolvedor parar o projeto ou uma empresa pedir falência, qualquer empresa que utiliza o aplicativo pode dar continuidade no projeto. Isto é possível através da contratação de um programador ou de uma empresa de desenvolvimento.

5.6 Motivação para Uso do Código Aberto

Iniciativas para a utilização de aplicativos com o código fonte aberto devem ser incentivadas, principalmente, quando realizadas na área de segurança. Atualmente esse tipo de aplicativo está sendo utilizado por empresas de quase todas as áreas existentes, senão todas. Grandes empresas, desenvolvedoras e apoiadoras do uso de programas proprietários, aderiram ao uso desses tipos de aplicativos, como é o caso da IBM[SEC 00].

No Brasil, a utilização de aplicativos com código fonte aberto ainda não é uma realidade. Grandes empresas ainda criam uma certa resistência ao uso desse tipo de programa, baseando-se em afirmações inverídicas, que declaram impossibilidade de responsabilizar empresas caso ocorra algum problema no aplicativo, ou que não há o

suporte necessário.

O próprio governo federal que deveria ser um exemplo para o país e apoiar situações como essa que oferecem muitas vantagens aos seus usuários, continua a apoiar e gastar quantidades exorbitantes do dinheiro público em licenças de aplicativos com código proprietário.

O custo não é o maior problema em um governo federal utilizar aplicativos com código fonte proprietário. Um órgão que possua dados importantes como o governo federal não deve, ou ao menos não deveria, utilizar um aplicativo que o seu operador, ou alguém do governo, não possua garantias das funções que ele está executando.

Divergindo do governo federal, já estão surgindo projetos de apoio aos aplicativos com o código fonte aberto, como é o caso do Rio Grande do Sul, onde em todos os órgãos do estado são utilizados esses aplicativos. Além disso, todos os projetos do governo na área de informática utilizam computadores com esse tipo de programa instalado.

A Infra-estrutura de Chaves Públicas é o maior projeto na área de segurança que Brasil possui atualmente. Um projeto desse porte não pode ficar dependente dos interesses de poucas pessoas ou de uma empresa. A melhor maneira de não criar esta dependência seria o uso de aplicativos com o código fonte aberto.

A segurança lógica do projeto estaria assegurada, pois a possibilidade de auditoria do código dos programas utilizados aumentaria a confiança das pessoas em relação ao seu uso. O uso desse tipo de programa em um projeto importante poderia abrir precedentes para uma posterior abertura do governo em relação aos aplicativos com código fonte aberto.

5.7 Conclusão

Aplicativos com o código fonte aberto já são uma realidade no mundo corporativo atual. O uso desse tipo de aplicativo está crescendo a cada dia que passa. Seu volume de crescimento tende a aumentar ainda mais no momento que as empresas compreenderem as inúmeras vantagens advindas desses aplicativos.

A visualização do código fonte é uma garantia de segurança que as empresas não possuem atualmente através do uso de aplicativos proprietários. Além disto, os aplicativos com o código fonte aberto trazem outras vantagens já detalhadas nesse capítulo, como características de personalização, maior suporte técnico, etc.

Capítulo 6

Modelos de ICP Implementados

6.1 Introdução

Este capítulo descreve o modelo de ICP descrito na medida provisória número 2.200-2, editada em agosto de 2001 pelo governo brasileiro e também alguns modelos de ICP implementados em outros países.

A estratégia é estudar os diferentes modelos implementados em lugares e situações distintas. A análise permitirá uma visão dos modelos utilizados em casos específicos, possibilitando a realização de um estudo para a obtenção de parâmetros para determinar o modelo ideal para a realidade brasileira.

A seção 6.2 comenta a proposta de ICP do governo brasileiro. A seção 6.3 descreve o modelo de ICP criado por um grupo de universidades e empresas européias. A seção 6.4 demonstra a ICP organizada pelo governo do Canadá. A seção 6.5 apresenta a estrutura proposta pelo governo federal dos Estados Unidos. Finalmente, a seção 6.6 apresenta uma comparação dos modelos descritos neste capítulo.

6.2 Proposta para o Modelo Brasileiro

Em 24 de agosto de 2001, o governo brasileiro editou a medida provisória número 2.200-2 instituindo a Infra-estrutura de Chaves Públicas Brasileira(ICP-

Brasil). Com a ICP-Brasil o governo quer garantir a autenticidade, integridade e validade jurídica de documentos assinados digitalmente[BRA].

O governo definiu um órgão chamado Comitê Gestor da ICP-Brasil como autoridade gestora de políticas da ICP-Brasil. Este comitê é composto por cinco membros da sociedade que trabalham em setores interessados na implementação da ICP-Brasil e um representante de cada um dos órgãos abaixo:

- Ministério da Justiça;
- Ministério da Fazenda;
- Ministério do Desenvolvimento, Indústria e Comércio Exterior;
- Ministério do Planejamento, Orçamento e Gestão;
- Ministério da Ciência e Tecnologia;
- Casa Civil da Presidência da República;
- Gabinete de Segurança Institucional da Presidência da República.

O comitê será responsável pela implementação e manutenção da ICP-Brasil. Também é sua responsabilidade a definição de políticas e regras operacionais da AC-Raiz e dos níveis abaixo.

O governo também definiu o Instituto Nacional de Tecnologia da Informação (ITI) como AC-Raiz da ICP-Brasil.

O modelo escolhido para a ICP-Brasil é baseado no modelo isolado, porém, no momento que forem estabelecidos contratos com empresas internacionais o modelo transformar-se-á em floresta. A ICP-Brasil é demonstrada na figura 6.1.

O modelo brasileiro está organizado da seguinte forma: no topo da hierarquia encontra-se a AC-Raiz. Toda a manutenção desta autoridade é tarefa do Comitê Gestor da ICP-Brasil. A função da AC-Raiz é emitir, expedir, distribuir, revogar e gerenciar os certificados digitais das AC de nível subseqüente ao seu. A AC-Raiz também é responsável pela fiscalização e auditoria das AC e AR autorizadas por ela a prestar

serviços em território nacional. Não é permitida a emissão de certificados digitais para usuários finais pela AC-Raiz.

Para uma AC ser credenciada pela ICP-Brasil, ela necessita antes ser totalmente auditada e deve estar de acordo com as regras definidas no documento Declaração de Regras Operacionais. Uma AC intermediária não pode certificar outra AC sem a prévia aprovação do Comitê Gestor da ICP-Brasil.

Documentos eletrônicos assinados por AC não integrantes da ICP-Brasil serão considerados válidos se forem admitidos como válido por ambas as partes ou aceito pela pessoa que se opor ao documento.

A Medida Provisória permite a integração da ICP-Brasil com ICP estrangeiras utilizando certificação cruzada. Para isto é necessário um acordo com a entidade internacional.

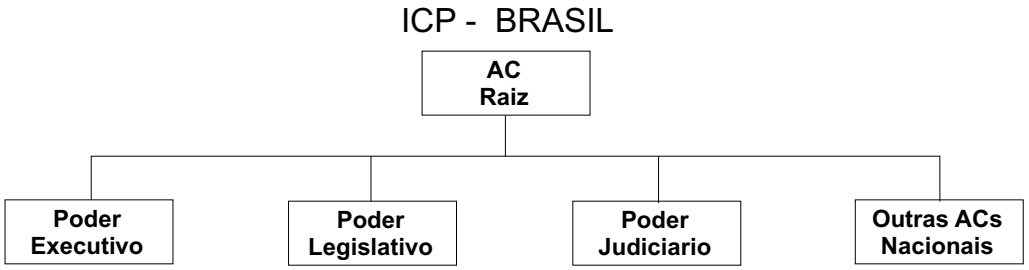

Figura 6.1: A ICP-Brasil define uma AC Raiz gerenciada por um comitê formado por membros, em grande parte, do Poder Executivo brasileiro. Abaixo da AC-Raiz estarão as AC dos três poderes brasileiros e das entidades privadas que desejam vincular-se a ICP-Brasil.

6.3 EuroPKI

A EuroPKI implementou uma estrutura para fornecer serviços de certificação de chaves públicas para indivíduos, organizações e projetos europeus. A EuroPKI não possui nenhum relacionamento com os governos europeus. O projeto é uma parceria entre universidades e organizações que possuem sua base na europa. A EuroPKI fornece uma maneira destas organizações e universidades estudarem as tecnologias de certificados digitais, além de poderem certificar digitalmente seus projetos. O modelo adotado pela

EuroPKI é mostrado na figura 6.2.

Grande parte da estrutura da EuroPKI está localizada dentro da Itália, onde está dividida em diferentes universidades.

O modelo adotado é baseado no Modelo Isolado. O modelo europeu possui uma AC-Raiz e todas as outras AC estão abaixo dela. Para o controle da AC-Raiz foi criada uma organização sem fins lucrativos também denominada EuroPKI. A criação de uma organização desse tipo garante a idoneidade da AC-Raiz.

A EuroPKI também define uma política para as AC e AR que desejam ocupar o nível imediatamente abaixo da AC-Raiz. Nela são definidas as obrigações assumidas pelas AC e AR após a sua integração à ICP.

Apesar da EuroPKI fornecer suporte para certificação cruzada, este recurso não foi utilizado ainda[DER].

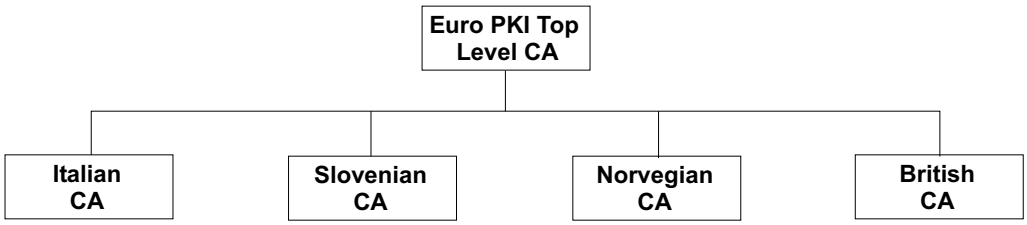

Figura 6.2: A EuroPKI é uma instituição sem fins lucrativos criada para gerenciar um projeto de ICP usado por várias organizações européias. A maioria das autoridades credenciadas à EuroPKI são universidades e companhias privadas localizadas na Europa. A EuroPKI segue o Modelo Isolado.

6.4 Modelo Canadense

Com o objetivo de aumentar o uso do comércio eletrônico nacional e internacional o governo federal do Canadá implementou uma Infra-estrutura de Chaves Públicas nacional. O governo também deseja utilizar a ICP como maneira para incentivar as empresas, que ainda utilizam outras formas de comércio, a usarem o comércio eletrônico.

Com a ICP, o governo canadense pretende integrar várias tecnologias usadas por ele para gerenciamento de informações e aplicações de comércio eletrônico.

A integração assegurará a segurança de uma grande quantidade de aplicações, não necessitando assim diferentes mecanismos de segurança para cada aplicação[dC 98].

A ICP do governo canadense é ilustrada na figura 6.3. Ela é composta dos seguinte componentes:

- Autoridade de Gerenciamento de Políticas (AGP);
- AC Central (ACC);
- AC;
- Autoridades de Registro Locais.

A Autoridade de Gerenciamento de Políticas é presidida pela Secretaria do Tesouro. O papel da AGP é fiscalizar o desenvolvimento das políticas que serão incluídas na ICP federal.

A AC Central é a AC que implementa as políticas definidas pelo governo e aprovada pela AGP. A ACC é, também, o ponto comum para organizações que desejam estabelecer certificação cruzada com a ICP do governo federal. O governo canadense permite certificação cruzada com empresas de setores privados nacionais. Departamentos do governo nacional e organizações internacionais também podem estabelecer certificação cruzada com o governo canadense.

As AC abaixo da ACC são operadas pelos departamentos dentro do governo. Cada AC é responsável pelo gerenciamento dos certificados digitais emitidos e, pelas AC e autoridades de registro subordinadas.

Todos os protocolos e algoritmos usados na ICP do governo canadense são baseados em padrões comerciais abertos.

6.5 Modelo Federal dos Estados Unidos

O intuito de criar uma ICP Federal nos Estados unidos é conseguir uma forma dos departamentos estaduais interagirem entre eles, e com agências nacionais. Ou-

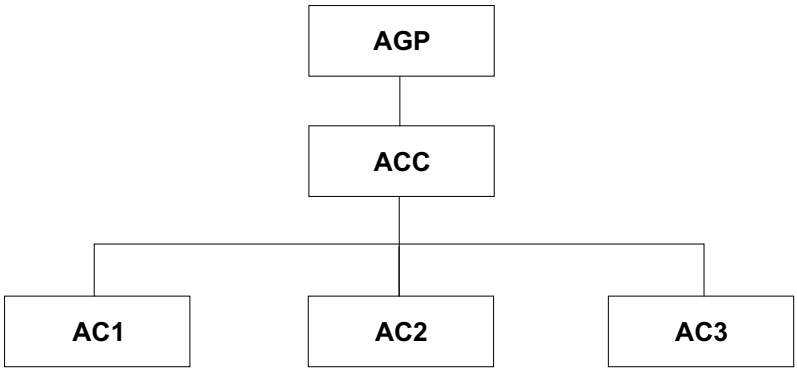

Figura 6.3: O Canadá criou uma ICP para facilitar o comércio eletrônico no país. A ICP canadense permite que entidades privadas do Canadá optem por serem subordinadas de uma AC sobre o domínio do governo federal, denominada AC Central, ou realizem certificação cruzada com ela.

tro propósito da ICP é fornecer formas seguras de comércio eletrônico utilizando a tecnologia Internet.

As agências norte-americanas são contra a criação de uma única AC Raiz em nível federal. As agências não admitem participar de uma ICP, cuja a AC-Raiz não esteja sobre seu controle. Elas alegam, também, que a criação de uma ICP única não atende aos requisitos de todas as ICP.

Para satisfazer todos os requisitos impostos pelas agências nacionais e estaduais norte-americanas, a solução encontrada foi a criação de uma AC Ponte. Esta AC não opera como uma AC raiz, pois ela não emite certificados para AC subordinadas. Seu método de operação é criar certificações cruzadas com cada entidade participante[ALT 01].

A AC Ponte também permite a criação de certificações cruzadas com AC comerciais.

Um outro modelo que poderia ser utilizado para atender as necessidades norte-americanas é o modelo em Malha. Este modelo não foi implementado devido ao número de agências que farão parte da ICP. O gerenciamento do modelo em Malha seria impossível.

6.6 Paralelo dos modelos

O capítulo descreveu quatro situações distintas onde estão sendo implantadas Infra-estruturas de Chaves Públicas. Cada caso possui características próprias e cada um optou pela escolha do modelo que os responsáveis pensavam condizer com suas necessidades.

A tabela 6.6 descreve as características próprias de cada modelo explicado nesse capítulo.

Tabela 6.1: A tabela ilustra as características próprias dos modelos implementados em diferentes países.

Local	Características
ICP-Brasil	Todas entidade nacionais devem estar abaixo de uma AC-Raiz única; Certificação cruzada não é permitida para entidades nacionais; Certificação cruzada é permitida para entidades estrangeiras; Órgão definido pelo governo é responsável pela AC-Raiz;
EuroPKI	Adoção do Modelo Isolado; Não há restrição para entidades quanto a certificação cruzada; Foi criada uma organização sem fins lucrativos para controlar a AC-Raiz;
Canadá	Utiliza o Modelo em Floresta com uma ICP do governo como ponto central; Possui uma Autoridade responsável pela definição e gerenciamento de políticas; Entidades nacionais, internacionais e governamentais podem estabelecer certificações cruzadas sem restrições;
Estados Unidos	O governo dos Estados Unidos está criando uma entidade para fazer o papel de Ponte; ICP comerciais e governamentais usarão certificação cruzada para conectar-se com a Ponte; Agências nacionais não aceitaram ficar abaixo de uma AC-Raiz controlada pelo governo;

6.7 Conclusão

Existem, atualmente, uma variedade de modelos de ICP que podem ser implementados em uma organização ou governo. Os responsáveis pela implementação devem definir o melhor modelo baseado em sua estrutura organizacional.

A necessidade de expansão e ligação com outras ICP também devem ser levados em consideração no momento da escolha do modelo.

Capítulo 7

Aplicações que Suportam Certificados Digitais

7.1 Introdução

Neste capítulo será mostrado alguns protocolos e aplicações que podem fazer uso de um certificado digital emitido por uma ICP, demonstrando assim, a importância da implantação de uma ICP no Brasil. Através do uso de certificados digitais, será possível a utilização de muitos serviços, necessários para garantir a segurança das pessoas e das redes.

O capítulo também aborda os projetos que estão sendo desenvolvidos pelo LabSEC e utilizam certificados digitais.

A seção 7.2 explica o protocolo utilizado para transferência de mensagens eletrônicas seguras. A seção 7.3 descreve o protocolo SSL utilizado para a criação de uma conexão segura entre uma máquina cliente e um servidor. A seção 7.4 discorre sobre o WTLS, protocolo utilizado para o estabelecimento de conexões seguras com dispositivos móveis. A seção 7.5 aborda o protocolo de segurança da camada IP, o IP-SEC. A seção 7.6 comenta a especificação SET. Finalmente, a seção 7.7 descreve alguns projetos criados pelo LabSEC que fazem uso de certificados digitais.

7.2 S/MIME

O *Secure/Multipurpose Internet Mail Extension* (S/MIME) é um incremento na parte de segurança do MIME, formato padrão de mensagens de correio eletrônico[STA 99].

O MIME é uma extensão da RFC 822, a qual define o formato das mensagens de texto que são enviadas através do correio eletrônico. O objetivo do MIME é suprir algumas limitações do SMTP e do formato definido na RFC 822.

O MIME insere um cabeçalho com o formato da mensagem, o qual deve ser interpretado pelo aplicativo que irá recebê-la. O S/MIME define algumas tipos novos de cabeçalhos utilizados em mensagens protegidas, funções não existentes no MIME. Os novos tipos utilizam os padrões PKCS #7 e PKCS #10, os quais foram descritos nas seções 3.7.1 e 3.7.2.

Utilizando o S/MIME é possível assinar uma mensagem de correio eletrônico. A verificação da assinatura é possível através do uso de qualquer aplicativo que suporte S/MIME.

Caso alguém queira enviar uma mensagem em segredo, o S/MIME possui uma função que cifra os dados da mensagem para uma ou mais pessoas autorizadas a lerem a mensagem.

O S/MIME também permite que uma mensagem seja assinada e cifrada.

7.3 SSL

O *Secure Socket Layer*(SSL) é um protocolo que fornece um canal de comunicação seguro entre duas máquinas. Ele protege os dados em trânsito e identifica a máquina que você está comunicando[RES 01].

O SSL foi inicialmente desenvolvido pela Netscape e inserido em seu navegador. Atualmente, a IETF assumiu o projeto e mudou seu nome para TLS.

Através do protocolo SSL é possível garantir os serviços de autenticação, integridade e confidencialidade. A confidencialidade dos dados é executada de modo

transparente para o usuário.

A autenticação no SSL pode ser feita de duas maneiras: unilateral ou mútua. A autenticação unilateral é quando somente o servidor autentica-se, dessa forma podemos garantir a autenticidade de um site, mas não é possível identificar a pessoa que está acessando. Na autenticação mútua ambas as partes são identificadas durante a conexão, desse modo é possível identificar a autenticidade de um site e, também, do cliente que está navegando nele.

Vários protocolos que são executados na camada TCP trabalham em conjunto com o SSL, é o caso do HTTP, SMTP, etc..

7.4 Dispositivos Móveis

As especificações dos protocolos que serão utilizados para garantir a segurança de dispositivos móveis é definido pelo WAP Forum. O WAP Forum é formado por indústrias interessadas no crescimento do setor de telefonia e na transmissão de informações em dispositivos móveis.

O WAP Forum definiu uma ICP para dispositivos com suporte ao protocolo WAP com o objetivo de reutilizar os padrões de ICP existentes, somente desenvolvendo novos padrões quando existir a necessidade de suportar requisitos específicos do WAP. O modelo de ICP para o protocolo WAP provê compatibilidade entre seus componentes e os componentes definidos para uso na Internet[FOR 01a].

O protocolo WAP possui uma camada para prover a segurança de uma comunicação utilizando dispositivos móveis. A camada de segurança da arquitetura WAP é chamada WTLS. O principal objetivo da camada WTLS é fornecer confidencialidade, integridade e autenticação das partes durante uma comunicação.

O WTLS possui funcionalidades similares ao SSL, incorporando novas características como suporte a datagramas, troca de chaves otimizadas e atualização dinâmica das chaves. O WTLS deve ser otimizado devido a baixa largura de banda que o protocolo WAP disponibiliza e a menor capacidade de processamento dos dispositivos móveis[FOR 01b].

7.5 IPsec

O *IP Security* (IPSEC) oferece suporte a serviços de segurança na camada de rede (IP). O IPSEC permite que um sistema defina o protocolo de segurança e o algoritmo que será usado.

O IPSEC é utilizado para a criação de Rede Privadas Virtuais, as quais permitem que usuários estabeleçam uma conexão segura utilizando redes públicas, por exemplo, a Internet.

Dois protocolos são definidos pelo IPSEC, sendo que o sistema deve escolher qual deles utilizará durante a conexão, os quais são: Authentication Header (AH) e Encapsulating Security Payload (ESP). O protocolo AH fornece suporte a integridade e autenticação dos pacotes IPs. O protocolo ESP provê os serviços de confidencialidade, podendo também utilizar o serviço de autenticação do protocolo AH.

O IPSEC fornece suporte ao uso de certificados digitais no formato X.509v3 para a troca de pacotes autenticados e/ou cifrados. Uma rede privada virtual deve estar com ambas as partes certificadas para garantir os serviços de autenticação e confidencialidade.

7.6 SET

O SET é um conjunto de especificações técnicas na área de segurança, desenvolvidas pela Visa e Mastercard com o objetivo de assegurar transações com cartões de crédito na Internet.

O SET permite que uma estrutura para pagamento, usando cartões de crédito, opere de modo seguro sobre uma rede pública. Para garantir a segurança, criptografia e certificados digitais são utilizados. Através do uso de certificados digitais todos os componentes que participam da transação podem ser autenticados pelo sistema, e possuem garantias de que as mensagens estão sendo trocadas de maneira confidencial.

A grande vantagem do SET é o não-conhecimento do número do cartão de crédito do cliente, por parte da empresa onde a compra está sendo realizada. Através

disto, muitos problemas de segurança são evitados como, por exemplo, o armazenamento de modo inseguro dos números de cartões de crédito dos clientes, o vazamento de informações sigilosas através dos funcionários das empresas, etc.

7.7 Projetos do LabSEC

O LabSEC/UFSC possui vários projetos que usufruirão dos recursos advindos da tecnologia de certificados digitais. Esses projetos surgiram juntamente com o LabSEC e, atualmente, ganharam repercussão em nível nacional.

Cada projeto possui um aluno de mestrado coordenando e vários bolsistas da graduação na execução das tarefas.

7.7.1 Cartório Virtual

O cartório virtual é uma tentativa de colocar os serviços oferecidos por um cartório tradicional disponíveis na Internet. Cada cartório tradicional deve possuir um site na Internet para disponibilizar serviços para os seus clientes. Alguns serviços obrigam a presença física do indivíduo, porém muitos deles podem ser efetuados totalmente pela Internet.

Toda a parte de autenticação dos envolvidos na transação e de validação de documentos são efetuadas através do uso de certificados digitais pelas partes envolvidas [DAN 01].

7.7.2 Votação Digital

O projeto sobre a votação digital possui um enfoque tanto em votação eleitoral como em votações para tomadas de decisões dentro de uma empresa. Na primeira etapa, foi definido um protocolo para a troca de dados de forma segura entre os vários sistemas que compreendem o projeto.

O projeto também define a arquitetura considerada ideal para a implementação de um sistema de votação digital.

O protocolo definido engloba todas as etapas da votação digital, atendendo os requisitos de segurança necessários para que o processo seja realizado com sucesso[ARA 02, DEV 01].

7.7.3 LabSEC Signer

O LabSEC Signer é um projeto que foi dividido em três módulos de estudos separados, para facilitar o seu desenvolvimento. O objetivo do LabSEC Signer é propor maneiras alternativas de proteger sua chave privada para realizar a assinatura digital de um documento.

No módulo 1 a chave privada é armazenada dentro de um Cartão Inteligente. Este cartão possui um processador interno e, a partir do momento que a chave é armazenada dentro do cartão não é mais possível retirá-la de lá, ou mesmo visualizá-la. Isto é possível graças ao poder de processamento do cartão, que executa tudo internamente. Além disto o cartão possui um número de identificação pessoal necessário para utilizá-lo.

O módulo 2 utiliza um leitor de impressão digital para a assinatura digital de algum documento. Esse módulo utiliza a impressão digital do indivíduo para cifrar a chave privada. Desta maneira sua utilização só é possível a partir do momento que o sujeito coloca seu dedo no leitor biométrico.

O módulo 3 usa um método pouco conhecido no atual estágio dá área de segurança. Ele utiliza um dispositivo chamado *Signpad* para compreender certas medidas biométricas de uma assinatura manual efetuada com uma caneta especial. O Signpad detecta a velocidade, pressão e posição da assinatura manual do indivíduo. Através de um cálculo efetuado sobre estas medidas, o *Signpad* extrai um valor que será utilizado na cifragem da chave privada. A chave privada só será decifrada através de uma nova assinatura realizada no *Signpad*.

7.7.4 Prontuário Médico Universal

O prontuário médico universal é um projeto que visa agilizar a consulta de médicos ao prontuário dos pacientes. Desta forma o projeto define um banco de dados, centralizado ou distribuído, que conterá as fichas médicas de todos os pacientes.

Os dados dos pacientes seriam divididos e classificados com um nível de segurança. Assim, alguns dados podem ser disponíveis para todos os usuários da Internet, outros podem ser disponíveis para pesquisadores e outros somente para o médico responsável.

Para garantir a segurança dos dados certificados digitais contendo o nível de autenticação são utilizados. Através de uma análise do certificado do cliente, o sistema disponibilizaria as informações adequadas.

Um sistema como esse traria uma organização maior para os sistemas utilizados em hospitais, além de fornecer meios para novos estudos por causa da estrutura de dados única.

7.7.5 Protocolizadora Digital de Documentos Eletrônicos

A Protocolizadora Digital de Documentos Eletrônicos (PDDE) é um sistema que cria um protocolo seguro para entrega de documentos eletrônicos[1]. A protocolizadora é um dispositivo baseado em aplicativos que recebe o documento em forma eletrônica e emite um recibo também em forma eletrônica comprovando a transação.

O grande diferencial desta protocolizadora são as garantias de segurança de todo o processo. Todos os dados armazenados e emitidos para o cliente pela protocolizadora são assinados digitalmente, o que garante a autenticidade.

Além disto, os aplicativos da protocolizadora garantem que, mesmo que ela seja uma entidade maliciosa, ela não poderá alterar o protocolo. Desta forma o cliente possui garantias da integridade do processo como um todo[PAS 02].

[1]O LabSEC/UFSC tem um convênio de transferência tecnológica deste projeto para a empresa de base tecnológica Bry Tecnologia S.A. (http://www.bry.com.br)

7.7.6 Sistema de Crédito Seguro

O Sistema de Crédito Seguro busca solucionar eventuais problemas de segurança nos sistemas eletrônicos de análise de créditos. O sistema definiu um protocolo, denominado I2AC, porque o simples uso de cifras simétricas e assimétricas não atendiam a todos as necessidades de segurança.

O protocolo I2AC garante que uma transação seja realizada de maneira totalmente confiável, mesmo que alguma entidade participante do processo queira agir de maneira maliciosa.

O protocolo faz uso de outro protocolo, o SSL (explicado na seção 7.3), para garantir os serviços de autenticação, integridade e confidencialidade[BRO 01].

7.7.7 Telefone e Fax Seguro

Estes sistemas objetivam estabelecer uma conexão segura através de linhas telefônicas convencionais. Para ambos os sistemas estão sendo projetados aparelhos especiais, que utilizarão certificados de chaves públicas para estabelecer a comunicação.

Os aparelhos utilizarão uma freqüência pré-determinada onde serão trafegados os dados cifrados. A amplitude atual já inclui essa freqüência, porém ela não é utilizada.

Os usuários dos aparelhos poderão escolher o momento em que desejam iniciar uma conexão segura. A partir disto, o sistema fará o processo de trocas de chaves públicas e começará a cifrar os dados.

7.7.8 Sistema de Atendimento ao Cliente Seguro

Garantir uma qualidade aceitável nos serviços de atendimento ao cliente é um problema para grande parte das empresas atualmente. Porém o Sistema de Atendimento ao Cliente Seguro busca resolver esse ponto falho.

Para resolver isso foi criado um protocolo. Ele engloba todas as fases do sistema, que vai desde o momento da ligação do cliente, passando por todos os problemas

possíveis, até que a soluçao seja encontrada.

Algoritmos criptográficos foram utilizados na elaboração do protocolo para garantir todos os requisitos necessários nas transações[GHI 02].

7.7.9 Segurança na Avaliação Não-Presencial

A Internet é muito usada para a realização de cursos a distância, como a intenção de agregar novos conhecimentos a profissionais de empresas e alunos em geral. Uma das etapas fundamentais de qualquer curso é a avaliação dos participantes, conhecendo-se assim, se o objetivo do ensino foi alcançado com sucesso.

O projeto focou-se nos problemas, relativos a segurança, que são encontrados em um processo de avaliação não-presencial, propondo uma nova arquitetura que permita o uso da Internet como meio para esse tipo de avaliação[SCH 02].

7.7.10 Proteção de Software por Certificação Digital

A garantia do direito autoral sobre aplicativos de computação é, certamente, um dos maiores problemas da informática. Atualmente, a pirataria lesa milhares de produtores de aplicativos em todo o mundo, causando um prejuízo para empresas e fabricantes na casa de bilhões de dólares. Nada do que foi feito até agora teve uma eficácia real, nem mesmo as leis federais.

O projeto realizou um estudo sobre Infra-estrutura de Chaves Públicas e sua possível aplicabilidade para proteção de aplicativos usando certificados digitais. O propósito é condicionar o registro de um software ao certificado digital do usuário[ROC 01].

7.8 Conclusão

Nesse capítulo foram vistas várias aplicações que fornecem suporte a certificados digitais. O suporte para certificados digitais aumentará no momento que novos mecanismos de uso popular forem portados para a Internet, como é o caso do cartório virtual.

Vários protocolos também já possuem suporte nativo para certificados digitais, incentivando seu uso em aplicações.

Os atuais aplicativos que oferecem suporte para certificados digitais possuem muitas incompatibilidades em relação ao que está descrito na recomendação X.509v3. Isso causa muitos problemas de compatibilidade entre os programas, causando transtornos para seus usuários.

Capítulo 8

Modelo Proposto

8.1 Introdução

A partir dos estudos realizados, foram encontrados muitos pontos que podem ser alterados ou aprimorados, nas Infra-estruturas de Chaves Públicas de uma maneira global, além de outras características que necessitam dessas mudanças para atenderem a necessidade específica de um contexto local.

O Brasil, assim como outros países, possui a necessidade de implantar uma ICP. Porém para garantir que ela atenda a todos os requisitos de segurança necessários e que não causará problemas no futuro, ela deve adequar algumas características para atender as necessidades dos cidadãos brasileiros e da estrutura do governo nacional.

Este capítulo detalha um novo modelo e características modificadas que podem ser mais adequadas às necessidades nacionais. O capítulo também aborda o uso de ferramentas baseadas em aplicativos com código fonte aberto, este tipo de metodologia atribui um nível maior de confiança por parte dos seus usuários.

A seção 8.2 teoriza sobre as vantagens da implementação de um novo modelo de ICP para o Brasil. A seção 8.3 descreve o uso de ferramentas com código fonte aberto para melhorar a confiabilidade do sistema. A seção 8.4 considera a descentralização de alguns componentes da ICP que ficam concentrados na AC e poderiam trabalhar de forma independente. A seção 8.5 aborda a inclusão de novos componentes para melhorar a

ICP como um todo, estes componentes podem criar novos serviços e melhorar a segurança de outros. A seção 8.6 ilustra uma nova característica que pode ser incorporada à emissão de certificados digitais. Finalmente, a seção 8.7 faz uma crítica ao modelo atual, que estabelece confiança para um conjunto de certificados sem informar os usuários.

8.2 Nova proposta: Modelo em Ponte

Após uma análise detalhada do modelo proposto pelo governo brasileiro e da avaliação dos modelos implantados em diversos outros países, concluiu-se que o modelo que o governo deseja implementar é inadequado à nação brasileira, tanto do ponto de vista organizacional quanto do estrutural.

O governo optou por um modelo tradicional, pensando em atender as suas necessidades internas. Porém, o modelo adotado dificultará a integração com outras Infra-estruturas de Chaves Públicas.

O modelo proposto pelo governo nacional também possui problemas em relação ao ponto de vista político pois, da maneira atual, uma ICP de um determinado grupo político pode ser obrigada a estar subordinada a outra ICP de um grupo político adversário.

8.2.1 Análise do Modelo Atual

O modelo de ICP que o governo deseja implantar está causando uma série de discussões, tanto políticas como operacionais. O governo brasileiro optou por um modelo simples baseado em uma hierarquia isolada(ver seção 3.8.1). Caso sejam fechados acordos com entidades de outros países, o modelo passará de uma hierarquia isolada para uma floresta de hierarquias(ver seção 3.8.1).

Esta política escolhida causará uma série de transtornos para as entidades nacionais que queiram filiar-se à ICP-Brasil. Seguindo isto, ao invés de incentivos, o governo brasileiro colocará uma série de barreiras para integração da área de segurança. De acordo com a MP 2.200, a única maneira de uma entidade nacional vincular-se a es-

trutura do governo seria submetendo-se as suas políticas e sendo vinculada abaixo dela, ou seja, deveria ser assinada ou pela AC-Raiz ou por alguma outra AC abaixo da Raiz.

Se uma ICP já possui sua estrutura montada, com uma AC-Raiz definida, assim como todo o restante da estrutura, para vincular-se a ICP-Brasil ela deverá promover uma série de mudanças que causará prejuízos para a instituição. Esta possui duas maneiras de integrar-se a estrutura do governo: criar duas estruturas totalmente independentes ou criar uma nova estrutura e migrar da antiga para a nova gradativamente. Em ambas as situações a empresa deverá arcar com custos operacionais e de equipamentos.

Enquanto todos esses transtornos são causados para a filiação de uma entidade nacional à ICP-Brasil, é permitido que as entidades internacionais estabeleçam certificações cruzadas diretamente com a AC-Raiz do modelo nacional. Isto proporciona um enorme favorecimento às empresas estrangeiras, pois elas poderão criar vínculos com a ICP nacional sem a necessidade de alterar em nada suas estruturas. Esta série de benefícios aumentará o número de clientes das ICP estrangeiras no país porque elas poderão oferecer seus serviços por valores menores, pois não precisarão pagar custos extras, o que ocorrerá com ICP legitimamente brasileiras. Como conseqüência disso pode haver um congelamento no crescimento desta área no mercado nacional.

O modelo atual também já está gerando uma série de discussões entre os poderes políticos nacionais. O Brasil dispõe de uma estrutura política formada por três poderes, sendo que a Constituição Federal de 1988, em seu artigo segundo, os declara *independentes e harmônicos entre si*.

O modelo proposto não segue o que está explicitado na Constituição Nacional, pois define uma entidade superior, a AC-Raiz. Os três poderes serão submetidos as suas políticas e determinações. A submissão a este órgão superior também pode causar problemas graves a qualquer um dos poderes, caso ela aja de forma maliciosa. Um exemplo disso seria a revogação do certificado de alguns dos poderes, depois de sua revogação o certificado não pode retornar ao estado válido. A única maneira de voltar a operar seria a emissão de um novo certificado, sendo que isto demandaria de tempo e causaria um grande transtorno.

O cenário proposto também pode causar problemas políticos pois o órgão administrador da ICP-Brasil é vinculado ao governo federal. Caso um governo estadual queira criar um estrutura e fazer parte da ICP-Brasil, ele pode ser prejudicado diretamente pelo governo federal. No caso do governo estadual ser filiado a um partido político diferente ao que o governo federal é filiado, o problema pode ter uma repercussão muito negativa.

8.2.2 O Novo Modelo

Este trabalho defende o ponto de vista de que o ideal para a atual estrutura organizacional brasileira é a adoção de um novo modelo baseado em uma entidade central, uma Ponte(ver seção 3.8.3). Este modelo já está sendo implementado nos Estados Unidos, e possui algumas características que podem evitar problemas futuros. Um exemplo da estrutura do governo brasileiro utilizando o Modelo com Ponte é ilustrado na figura 8.1.

8.2.2.1 Autonomia dos Poderes

A principal vantagem do uso do modelo em Ponte é que sua entidade central não pode ser considerado um órgão superior, como é o caso de uma AC-Raiz. Esta entidade simplesmente estabelece um modo das ICP conectadas a ela estabelecerem uma comunicação entre si.

Por causa disso, cada um dos poderes nacionais poderá ter sua própria estrutura, com uma AC-Raiz independente. Além disto, eles terão total liberdade para estabelecer suas próprias políticas, tendo validade apenas em sua hierarquia.

O modelo em ponte também gera uma liberdade para que cada uma das estruturas ligadas a ele possua um modelo diferente. Cada um dos poderes nacionais poderá adotar um modelo diferente de acordo com suas necessidades.

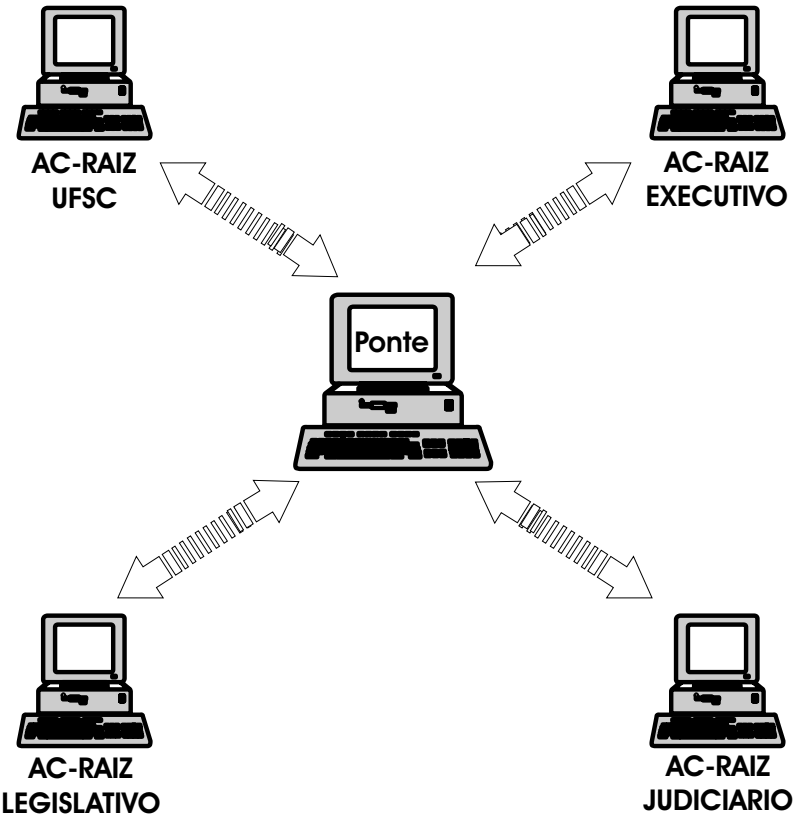

Figura 8.1: A figura ilustra a estrutura criada pelo governo utilizando um Modelo com Ponte, ao invés de uma hierarquia isolada.

8.2.2.2 Segurança

Como visto anteriormente, o Modelo em Ponte atribui uma independência para cada hierarquia ligada à entidade central. Isto evita problemas de segurança para as entidades associadas a ICP-Brasil.

Se a entidade central desejar agir de forma maliciosa, esta não pode causar danos graves a qualquer um dos órgãos ou empresas ligadas a ela. Independente do ato por ela cometido, as informações internas da hierarquia atingida continuarão trafegando normalmente. A ação da entidade maliciosa não causará nenhum risco à segurança das informações.

O fluxo de informações trocadas com outras hierarquias ligadas a ela através da ponte sofrerá uma interrupção até o descobrimento do problema. Porém o seu restabelecimento pode ser feito de forma simples e ágil, bastando apenas criar uma nova

certificação cruzada com a entidade central.

Um problema como o acima citado não afeta os certificados emitidos pela hierarquia atingida. Sendo assim, esses não necessitarão ser reemitidos após o problema. Isto é garantido pela independência de cada hierarquia.

8.2.2.3 Igualdade para as Empresas Nacionais

A implantação de um Modelo em Ponte traria uma série de benefícios para as empresas nacionais que desejam vincular-se à ICP-Brasil. Seguindo a MP atual, estas empresas possuem desvantagens em relação as estrangeiras.

Atualmente, somente empresas não-nacionais tem permissão para a criação de certificações cruzadas com a ICP-Brasil, sendo que as empresas nacionais devem estar abaixo dela. Como o modelo aqui proposto é totalmente baseado em certificações cruzadas, ambas as empresas estariam ligadas a estrutura nacional através desse tipo de certificação.

Com o uso do novo modelo, as empresas nacionais e estrangeiras possuirão os mesmos privilégios. Desta forma, nossas empresas podem oferecer serviços de certificação com a mesma qualidade por custos iguais ou até menores. Isto é garantido porque elas não terão gastos adicionais para sua inclusão na ICP-Brasil.

8.2.2.4 Administração Independente

Com o uso do modelo proposto a entidade central não possui privilégios para afetar a estrutura como um todo. Por causa desta característica, para administrar a entidade central poderá ser criada ou uma órgão não-governamental ou, até mesmo, um órgão do governo.

Independente do órgão responsável pela administração da entidade central, a liberdade dos três poderes nacionais estabelecida na Constituição está garantida.

8.2.2.5 Responsabilidade Total da Empresa

Para o correto funcionamento de um certificado digital e dos serviços por ele prestado, todos os dados necessários para a verificação do caminho de certificação devem estar presentes e atualizados corretamente.

Caso ocorra um problema com algum desses dados, o certificado digital será considerado inválido pelo sistema e não poderá ser utilizado.

Usando o modelo proposto, a entidade, seja ela nacional ou internacional, será totalmente responsável pela manutenção da estrutura e, na ocorrência de algum problema, o usuário do sistema poderá responsabilizar totalmente a empresa pelas suas perdas ou tempo de inoperância.

Se a empresa possuir um entidade externa influenciando neste processo, ela pode acusar essa entidade de estar causando os problemas. Isso pode ocorrer no modelo atual.

8.2.2.6 Problemas Políticos

Do modo como está organizada atualmente a ICP-Brasil todos os órgãos nacionais estarão abaixo da entidade administrada pelo poder executivo, dentre eles os governos estaduais e municipais.

O modelo em ponte possibilita que governos de partido diferentes ou até do mesmo partido criem estruturas separadas da ICP-Brasil. Desse modo, o governo federal não pode causar grandes prejuízos a uma estrutura estadual porque possuem pensamentos políticos distintos.

A estrutura proposta também não poderá ser utilizada como forma de pressionar os governos estaduais e municipais em decisões políticas.

8.2.2.7 Por que confiar no governo?

Por que uma entidade nacional deve confiar no governo federal? Este é o argumento mais utilizado nos Estado Unidos e que levou o governo americano a adotar uma estrutura na qual este trabalho foi baseado.

As entidades nacionais não deveriam ser obrigadas a confiar na idoneidade dos técnicos do governo federal. Da forma atual, a entidade nacional também deverá confiar na estrutura de segurança oferecida pelo governo.

Como falado na seção anterior, da forma como está, a estrutura atual pode ser usada como forma de pressionar entidades e fazê-las optar por uma alternativa de interesse do governo.

É possível argumentar que uma entidade nacional pode não ficar abaixo do governo federal e, mesmo assim, vincular-se a ICP-Brasil sendo assinada por um órgão internacional. Porém a entidade nacional ainda ficaria dependente de outro órgão, em que talvez também não queira confiar.

8.2.2.8 Ambiente de Segurança

O modelo proposto garante que cada empresa poderá criar e gerenciar seu próprio ambiente de segurança, obedecendo os requisitos mínimos exigidos pela ICP-Brasil.

A empresa poderá optar por possuir um sistema moderno e com características adicionais próprias que garantam um sistema de segurança mais eficiente para seus usuários, podendo, inclusive, utilizá-lo como ferramenta de publicidade para conquistar novos clientes.

Do modo como a ICP-Brasil está organizada atualmente desmotiva as empresas a investirem em seus ambientes de segurança. Mesmo que elas tenham um sistema diferenciado das outras, todas estarão ligados a mesma entidade superior, que possuirá uma única segurança. Se a entidade superior tiver algum problema de segurança ela prejudicará, da mesma forma, tanto a entidade inferior que possuir somente o padrão mínimo de segurança exigido pelo governo, como a entidade que tiver investimentos extras no seu ambiente de segurança.

8.3 Ferramentas com Código Fonte aberto

A partir do momento que um usuário possui um certificado digital, ele pode utilizar ferramentas para usufruir dos serviços que o certificado oferece. Porém, estas ferramentas devem seguir certos requisitos para que seu uso seja totalmente confiável.

Quando uma ferramenta visa oferecer segurança para os seus usuários, antes de tudo ela também deve oferecer garantias que possui tal segurança. As ferramentas de segurança atuais exigem que o usuário confie no desenvolvedor, pois ele recebe somente o código compilado, que não é compreensível.

Uma característica que as ferramentas dessa área devem oferecer é a capacidade de visualização do seu código, isto evita qualquer dúvida do usuário quanto a integridade do código. Além disto, evita que desenvolvedores mal-intencionados insiram códigos maliciosos com o intuito de prejudicar alguém ou alguma coisa.

A Internet está aumentando a visibilidade das ferramentas com código fonte aberto, mas cabe aos desenvolvedores adotar essa idéia e divulgar aos usuários suas vantagens. Uma excelente oportunidade para esta divulgação é a utilização delas em projetos importantes, como é o caso de uma ICP.

8.3.1 Metodologias de Uso

Atualmente, a grande maioria dos aplicativos que possuem suporte aos serviços oferecidos pelos certificados digitais são disponíveis por empresas desenvolvedoras. Estas empresas desenvolvem seus aplicativos seguindo suas próprias filosofias, as quais não são de conhecimento do usuário. Além disto, os aplicativos chegam ao usuário final já compilados, de maneira que o usuário possa apenas executá-los. Mas como os aplicativos são compilados, não há a possibilidade de acompanhar os passos que estão sendo executados, ficando o usuário obrigado a confiar na idoneidade da empresa.

Como o governo está criando sua própria ICP, o ideal seria que ele também desenvolvesse algumas ferramentas para garantir o uso correto dela. Esta garantia seria possível no caso do governo utilizar uma política de desenvolvimento de ferramentas com o código fonte aberto.

Dessa forma o governo poderia criar um sítio onde ficariam disponíveis todos os aplicativos desenvolvidos. Além do programa compilado para uso pelo usuário final, também seria disponibilizado o código fonte do aplicativo.

Utilizando esta metodologia, um usuário pode buscar o código fonte do arquivo no sítio, compilá-lo e executar a Função Resumo. O passo seguinte é baixar o aplicativo compilado e também executar a Função Resumo sobre ele. Após ele deve comparar o resultado da Função Resumo executada sobre o aplicativo obtido do código fonte e a executada sobre o aplicativo compilado.

Se o resultado for idêntico é assegurado que a versão compilada encontrada no sítio originou do código fonte lá disponível. Analisando o código fonte é possível afirmar que o aplicativo não possui nenhuma linha de código maliciosa com o intuito de confundir ou enganar o usuário.

Caso os resultados não sejam idênticos, o aplicativo compilado existente é resultado de outro código fonte, diferente do disposto pelo governo. Em razão disso, não seria aconselhável o uso do aplicativo, pois não é possível descobrir o que foi alterado em relação ao código fonte disponível. A figura 8.2 ilustra o processo para verificação da integridade de um aplicativo.

Os usuários, em sua maioria, não possuem capacidades técnicas para realizar os testes acima citados. Porém, possibilitará aos usuários que possuem conhecimentos suficiente realizem o processo e alertem os demais usuários sobre possíveis problemas nos aplicativos. Através disto, os usuários podem acompanhar o desenvolvimento das ferramentas pelo governo auxiliando na resolução de problemas.

O governo, além do desenvolvimento dos aplicativos, também deveria ser responsável pela manutenção da integridade do sítio e dos aplicativos lá encontrados, evitando assim que a análise do código fonte e verificação da Função Resumo necessitem ser realizadas em períodos de tempo extremamente curtos.

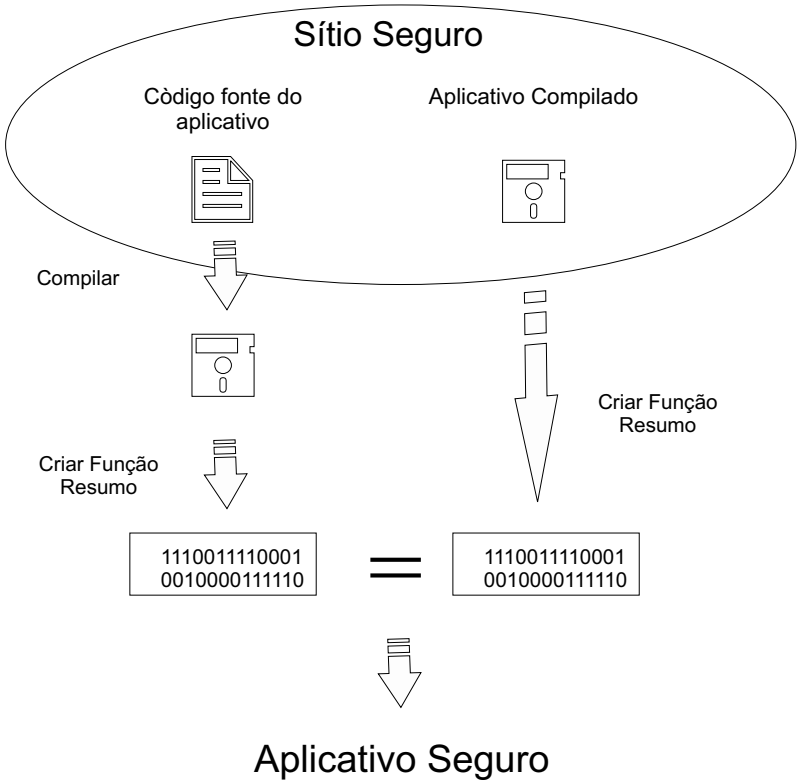

Figura 8.2: Para verificar se o aplicativo é seguro, o usuário deve baixar o código fonte e o aplicativo compilado do sítio específico. Após buscar os aplicativos, ele deve compilar o código fonte e executar a Função Resumo sobre ele. Depois deve executar a função resumo sobre o aplicativo que ele já buscou compilado. Se os resultados forem idênticos, o aplicativo compilado disponível tem origem do código fonte disponível.

8.3.2 Exemplos de Ferramentas

Uma ICP não é algo comum na vida da maioria dos cidadãos. Por isto o governo deve procurar maneiras de facilitar seu uso por parte dos usuários finais. O desenvolvimento de ferramentas que realizem os serviços básicos propostos seria uma maneira de incentivar o uso da ICP-Brasil. As ferramentas devem possuir uma interface amigável para que os usuários mais leigos possam utilizá-las sem maiores dificuldades.

Os aplicativos devem seguir os padrões mais utilizados na Internet, buscando oferecer uma compatibilidade com as ferramentas já existentes no mercado e outras que venham a ser desenvolvidas.

Serão descritas algumas ferramentas que o governo deveria, obrigatori-

amente, desenvolver. Elas realizam os principais serviços oferecidos pela ICP-Brasil.

Assinatura Digital de Documentos Eletrônicos Ferramenta que efetua a assinatura digital de um documento eletrônico. Ela permite ao usuário selecionar um documento em modo eletrônico e assiná-lo com seu certificado digital.

Verificação da Assinatura Digital Ela permite que o usuário verifique a assinatura digital de um determinado documento. O usuário selecionará o documento e a assinatura digital equivalente a ele. A ferramenta executará todo o processo para conferência da assinatura do documento e retornará se ela é válida ou não.

Verificação do Certificado Digital A ferramenta fará a verificação da validade do certificado digital e, também, do caminho de certificação. Para determinar se o certificado é válido, a ferramenta verificará o seu período de validade, ou seja, se não expirou. Além disto, o aplicativo consultará a última LCR e examinará se o certificado não está presente. O processo para verificação do caminho de certificação é o mesmo descrito na seção 3.9.

Cifragem de Documentos Eletrônicos Ferramenta usada para cifrar um documento eletrônico. Ela permite ao usuário escolher o documento que deseja cifrar e o certificado utilizado para o processo. O documento cifrado será gravado em um novo arquivo que pode ser enviado pela Internet ou armazenado em um computador.

Decifragem de Documentos Eletrônicos Ferramenta usada no momento que o usuário quiser decifrar um documento anteriormente cifrado. Ela permite selecionar o texto cifrado e o certificado que deve ser usado para a operação. A ferramenta retorna para o usuário o texto aberto resultante da operação.

Protocolização de Documentos Eletrônicos Através do uso desta ferramenta é possível a protocolização de um documento digital. Ela envia o arquivo para a Autoridade de Datação e recebe de volta um arquivo contendo um comprovante de que o processo foi realizado.

8.4 Descentralização de Componentes

Atualmente, muitas Infra-estruturas de Chaves Públicas mantém uma estrutura centralizada. Estas estruturas mantém a Autoridade Certificadora executando outras funções, além da simples emissão de certificados digitais.

Esta centralização pode, em alguns casos, diminuir a eficácia do componente que está sobrecarregado. Além disto, se acontecer algum problema com esse componente outros serão prejudicados.

8.4.1 Vantagens da Descentralização

No decorrer dos últimos anos, estudos vêm demonstrando que através do uso de estruturas descentralizadas, as empresas estão conquistando resultados positivos na organização como um todo. A descentralização de uma ICP também trará ganhos significativos para a estrutura, pois será possível definir as tarefas específicas de cada componente.

Grande parte dos modelos atuais já possuem estruturas parcialmente descentralizadas. Por exemplo, eles consideram a Autoridade de Registro um módulo independente da AC. Porém, a última ainda possui outros componentes vinculados a ela que poderiam ser separados.

Através da separação dos componentes, um processo tornar-se-á independente do outro. Desta forma, se ocorrer problema com um módulo, os outros poderão continuar executando suas tarefas. O protocolo X.509 v3 já possui suporte para a descentralização dos processos que, em muitos casos, continuam sendo executados pela AC.

Um exemplo de problema é o caso da AC sofrer algum dano. Caso ela seja responsável por outras funções como a revogação de certificados, esta parte também será afetada. Porém, se a revogação for efetuada por um componente diferente, ela não sofrerá interferência dos problemas da AC.

O uso de componentes desvinculados também pode trazer uma melhora na segurança da ICP. A separação possibilitaria que a AC permanecesse desconectada de

qualquer rede. Todavia, os outros módulo poderiam ser mantidos conectados em rede executando suas funções, sem comprometer o funcionamento da AC.

8.4.2 Autoridade de Revogação

A Autoridade de Revogação tem como sua principal função a capacidade de revogar certificados antes da sua expiração. Normalmente a revogação de certificados digitais é executado pela AC. Porém é possível a descentralização das funções, facilitando o balanceamento de tarefas entre os vários componentes de uma ICP[EUR].

Outra função de uma Autoridade de Revogação pode ser a centralização do controle de revogação de várias AC. Uma AC pode delegar a tarefa de revogação de seus certificados digitais para uma Autoridade de Revogação, liberando-se da realização desta tarefa. Dessa maneira, um conjunto de AC podem eleger uma Autoridade de Revogação para responsabilizar-se pela revogação de todos os seus certificados.

A Autoridade de Revogação não necessita pertencer a empresa, sendo possível criar uma entidade somente responsável pela revogação e publicação das listas de certificados revogados de várias AC. O exemplo de uma estrutura com várias Autoridades Certificadoras usando uma Autoridade de revogação é ilustrado na figura 8.3.

8.4.3 Autoridade de Políticas

Uma Autoridade de Política é responsável por estabelecer, atribuir e manter as políticas e procedimentos para todas as entidades da ICP. Ela deve estabelecer a função de cada componente de acordo com as políticas estabelecidas.

A Autoridade de Política também é encarregada da atribuição das políticas que serão inseridas em um certificado digital. Através destas políticas é possível determinar certas funções para um certificado digital e especificar o seu uso.

A Autoridade de Política recebe a requisição de certificado da AC e inclui as extensões e restrições necessárias para o certificado seguindo suas políticas. Quando o processo for finalizado, a estrutura do certificado é enviado de volta para AC, para

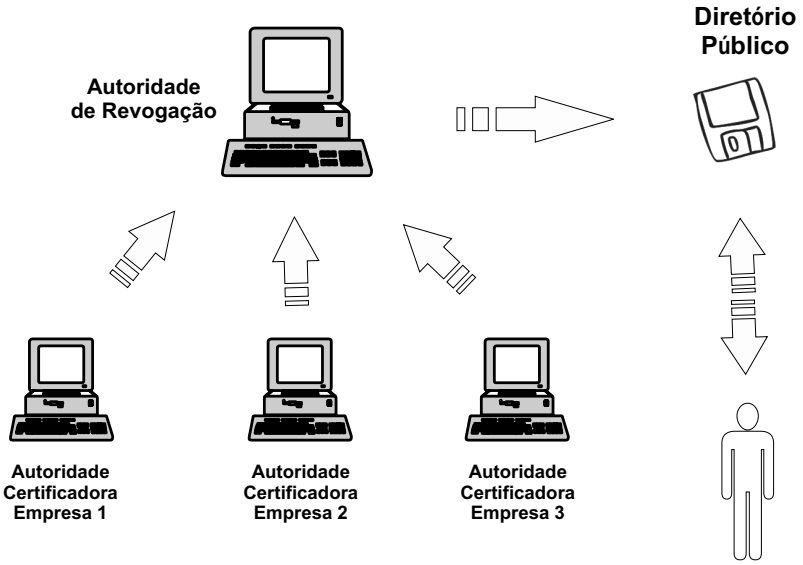

Figura 8.3: A figura ilustra o processo de revogação de certificados digitais com a utilização de uma única Autoridade de Revogação, responsável pela revogação dos certificados de várias Autoridades Certificadoras. A Autoridade de Revogação revoga os certificados e assina as listas de certificados revogados. Após as LCR são publicadas nos respectivos diretórios públicos. As entidades finais acessam estes diretórios para consultar as LCR e validar os certificados.

que esta assine o certificado digital. Uma estrutura simplificada utilizando uma Autoridade de Políticas é ilustrada na figura 8.4

A Autoridade de Política é encarregada de resolver disputas em relação a políticas e procedimentos[AUS 01].

8.5 Novos Componentes

Embora as Infra-estruturas de Chaves Públicas atuais forneçam boa parte dos serviços necessários, ainda é possível a inclusão de novos componentes com o objetivo de aumentar o número de serviços disponíveis. Além dos novos serviços, muitos outros poderão ter sua qualidade aprimorada.

Alguns desses componentes já existem na Internet, mas seus serviços são disponíveis independentemente das ICP. Colocando todos os componentes em um cenário único, cria-se um ambiente com um nível de segurança superior aos atuais. Al-

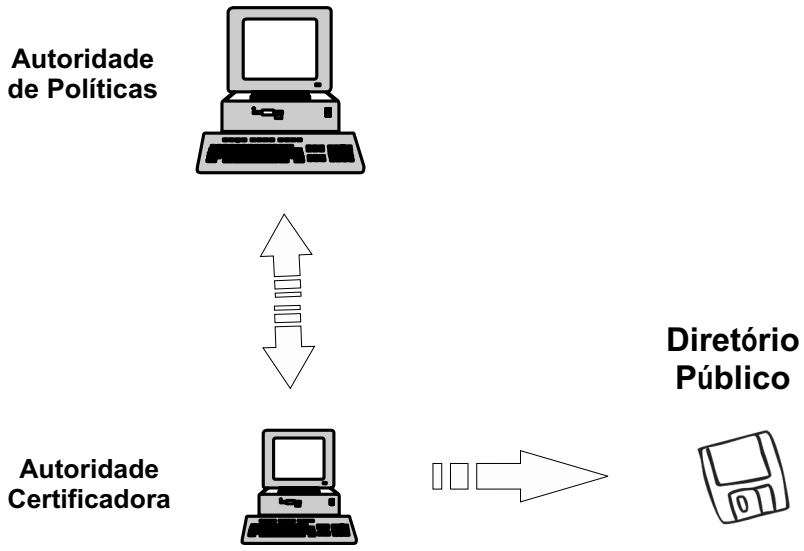

Figura 8.4: A figura ilustra o processo de emissão de um certificado com a inclusão de uma Autoridade de Políticas na ICP. A AC recebe a requisição e a repassa para a Autoridade de Políticas, esta insere as extensões necessárias e envia a estrutura do certificado para a AC assinar. Após a AC publica o certificado no Diretório Público.

guns componentes oferecem serviços individuais e independentes, ou seja, para obtermos uma melhor segurança é necessário aproveitar estas características de cada componente.

Se todos eles estiverem em um ambiente, executando seus serviços e aproveitando as características que os outros componentes oferecem, a qualidade do sistema será muito melhor que impossibilitar que um componente utilize os serviços de outros, ou ainda, delimitar que um componente possa utilizar os serviços de somente alguns dos outros existente na estrutura. Para disponibilizar todos os serviços, a ICP deve possuir um sistema com todos seus componentes integrados, porém eles não necessitam estar localizados em um mesmo ambiente físico.

Além disto, inserindo estes componentes à ICP é possível oferecer mais segurança de modo transparente e simplificado ao usuário, pois ele necessitará de uma única estrutura para utilizar todos os serviços que uma ICP pode oferecer.

8.5.1 Autoridade de Datação

Autoridades de Datação (AD) são necessárias para comprovar a existência de uma estrutura de dados em uma determinada data e hora. Uma AD recebe o Resumo da Mensagem assinado, concatena um ”carimbo” contendo a data e hora de recebimento e assina todo o conjunto.

Uma AD não deve ter conhecimento do conteúdo do documento que ela está assinando. Isto é assegurado através do envio do resultado da Função Resumo, juntamente com sua assinatura digital. Porém, a AD necessita assegurar que a assinatura digital do documento possui integridade e que o certificado que assinou é válido naquele momento [HAB 91]. Para garantir isto, são executadas as seguintes ações:

- A assinatura do resultado da Função Resumo é verificada utilizando a chave pública da entidade assinante;
- Se o certificado não está expirado, ou se não está presente na Lista de Certificado Revogados correspondente.

Uma AD também é usada para assegurar a ordem de recebimento de cada mensagem, isto é assegurado porque o resumo da mensagem é armazenado em uma base de dados. Com isto, é possível localizar a posição de cada mensagem e garantir que uma mensagem foi assinada antes de outra.

Isto é necessário no caso da necessidade de provar que uma mensagem foi enviada primeiro por certa entidade. Um caso onde haveria esta necessidade seria um leilão fechado, onde o maior lance ganha a preferência de compra. No caso de dois valores iguais, o primeiro valor é o beneficiado. A presença de uma AD seria crucial para a execução do leilão.

8.5.2 Autoridade de Aviso

A Autoridade de Aviso (AA) é responsável por toda comunicação oficial entre entidades. Se o processo normal de comunicação tiver problemas de recusa de recebimento (repúdio), ou seja, se uma entidade não conseguir uma resposta de outra,

ela deverá utilizar uma Autoridade de Aviso. A AA tem o dever de assegurar que um documento eletrônico foi entregue para determinada entidade ou pessoa [CUS 01].

A AA faz o papel do jornal ou de cartas registradas enviadas pelo correio. Ela pode enviar um e-mail, publicar o aviso em jornais on-line, fóruns, ou até mesmo em jornais de papel. Tudo o que for feito pela AA deve ser publicado em um diretório público.

Após executada a tarefa, a AA deve preencher um relatório, incluindo todos os passos realizados.

8.6 Controle de Datação em Certificados

O modelo atual não possui nenhum controle de datação no certificados digitais. A falta deste pode acarretar em problemas caso a entidade final e a Autoridade Certificadora façam um acordo tentando prejudicar um terceiro.

Utilizando os serviços prestados pela Autoridade de Datação é possível evitar esse tipo de problema, além de tornar possível uma fiscalização mais rígida do estado de um certificado em um determinado período do tempo.

Além disto, como os algoritmos utilizados pelas Autoridades de Datação não permitem que os dados sejam alterados por qualquer pessoa, mesmo os seus administradores, isto impossibilitará que essa autoridade faça parte de um acordo como mencionado acima.

8.6.1 Modelo atual

As Infra-estruturas de Chaves Públicas atuais não incluem datação em momento algum. Isto se deve, em grande parte, pelo não uso de AD dentro ou fora da sua estrutura. A datação de certas ações executadas pelos componentes de uma ICP pode evitar a ocorrência de problemas causados por pessoas que tenham atitudes maliciosas.

No modelo atual, a emissão de um certificado digital segue o seguinte processo: Em um primeiro momento é necessário o preenchimento dos dados no módulo

público. Após isto, é gerado o par de chaves, sendo que a privada permanece armazenada localmente, enquanto que a chave pública é inserida na requisição. Esta é enviada para a AR para conferência dos dados. Os dados são conferidos e a requisição é repassada para AC, que a assina. Após finalizado o processo, o certificado deve ser enviado para o Diretório Público e também para o sujeito. A figura 8.5 ilustra o processo de emissão de um certificado digital no modelo atual.

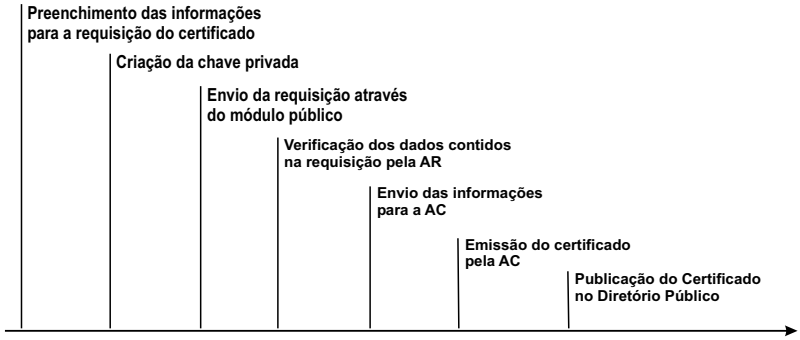

Figura 8.5: A figura ilustra os passos necessários para a emissão de um certificado digital. O usuário digita os dados no módulo público e os envia para a AR, esta confere os dados e retransmite-os para a AC que faz a assinatura. Após assinado o certificado é publicado no Diretório Público.

Como pode ser visto, não há registro de datação durante o processo de emissão de um certificado digital. Não é possível conhecer exatamente o momento em que ocorreu cada processo e nem o tempo decorrido entre eles. Um usuário, por exemplo, não pode garantir que a AC demorou mais tempo para emitir o certificado do que o especificado na Políticas de Certificação da empresa.

Da mesma forma que não existe controle algum sobre os eventos de uma requisição de certificado, isto também ocorre em um pedido de revogação.

Para efetuar a revogação de um certificado, o sujeito preenche um formulário no Módulo Público pedindo a revogação do seu certificado, esta solicitação é enviada para a AR que confirma sua validade. Após finalizado este passo, a solicitação é repassada para a AC, onde esta revoga o certificado. Após a LCR contendo a última revogação é publicada no Diretório Público. A figura 8.6 apresenta as etapas de uma solicitação de revogação de certificado.

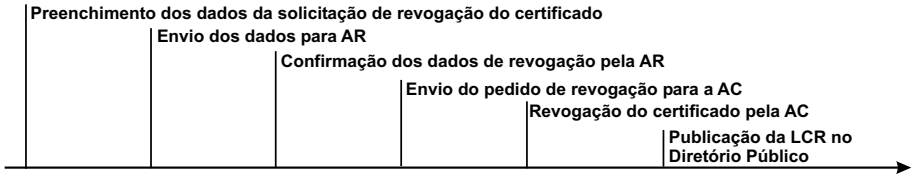

Figura 8.6: A figura ilustra os passos necessários para a revogação de um certificado digital. A solicitação de revogação é preenchida no Módulo Público e enviada para a AR. Esta confirma os dados e retransmite a solicitação para a AC, onde o certificado é revogado. Após concluída esta etapa a LCR atualizada é enviada para o Diretório Público.

A seguir é apresentado um exemplo de mau uso de uma ICP que não possua controle de datação: Uma pessoa do alto escalão de uma empresa transmite determinada ordem para seus subordinados a partir de uma mensagem assinada digitalmente. Caso as determinações passadas surtirem efeitos negativos para a empresa, a pessoa responsável pelas ordens erradas pode entrar em contato com o administrador da ICP. Através de um acordo, seu certificado é revogado com uma data retroativa a do documento assinado. Desta maneira, ausentaria o funcionário do alto escalão de qualquer responsabilidade sobre o documento mandado, alegando que sua chave privada estava ameaçada e ele revogou seu certificado antes da ação.

8.6.2 Modelo com Controle de Datação

O objetivo do controle de datação é obter um controle maior sobre cada evento de uma AC, assim como, por meio da inclusão de determinados registros em um certificado pode-se aprimorar a segurança do sistema como um todo.

Integrando uma AD no processo de emissão e revogação de certificados possibilitará que as etapas do processo sejam registradas. Se acontecer algum problema durante o processo será possível descobrir em qual etapa ocorreu a falha, assim como o momento exato.

O uso de uma Autoridade de Datação evitará que duas ou mais partes envolvidas em uma transação estabeleçam acordos tentando prejudicar alguém. Isto é possível porque os mecanismos que fazem a datação dos dados não permitem a inclusão de registros de forma retroativa. Deste modo, mesmo se a AD for uma entidade maliciosa,

ela não poderá agir de forma a prejudicar alguém, pois os seus mecanismos não permitem tal coisa.

Além dos registros gravados na AD, o sistema também pode incluir no certificado os registros de datação mais importantes. Um registro que deve ser incluído, por exemplo, no certificado é a data real de emissão do mesmo. O certificado já possui um campo com a data de emissão, porém este é baseado de acordo com o horário da AC, ou seja, o tempo que o relógio dela está marcando no momento da emissão. Se a AC for uma entidade maliciosa, ela pode atrasar ou adiantar seu relógio, visando prejudicar determinada entidade. Porém se no certificado constar o dia e hora do registro da AD, mesmo a AC agindo como entidade maliciosa e adiantando seu relógio, haverá um campo contendo a data exata da emissão. A figura 8.7 ilustra o processo de emissão de certificado com controle de datação.

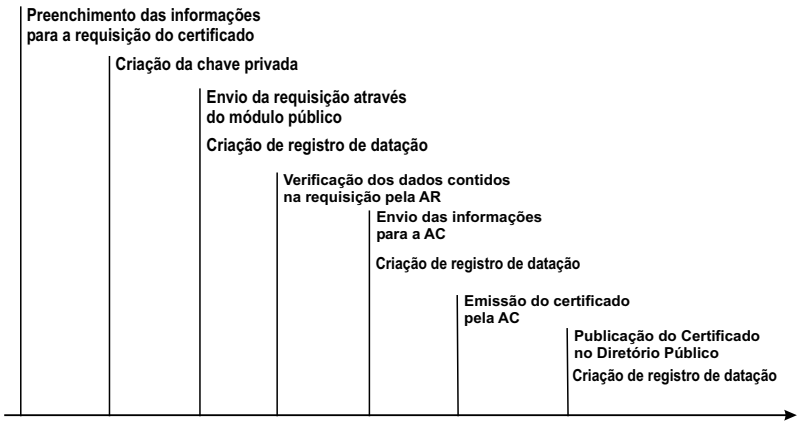

Figura 8.7: A figura descreve como seria o processo de emissão de um certificado digital usando um controle de datação. A cada troca de mensagem entre dois componentes é gravado um registro de datação. Com este dado é possível conhecer cada tarefa já realizada no processo e o tempo que levou para efetuá-la.

O processo de revogação de um certificado digital também pode usar uma AD para torná-lo mais seguro. Da mesma forma que utilizada na emissão de um certificado, a AD deve criar um registro de datação a cada momento que as informações são trocadas entre os componentes. Com isto é possível ter conhecimento do horário exato da revogação do certificado, não permitindo a AC mudar seu horário para a revogação de um determinado certificado visando beneficiar alguma das partes. A figura 8.8 ilustra

como deve ser a revogação de um certificado com controle de datação.

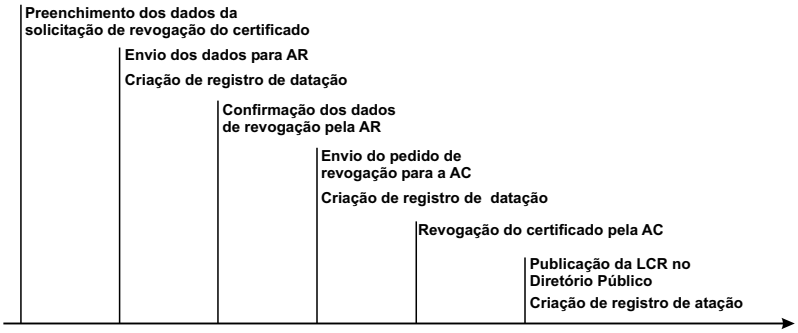

Figura 8.8: A figura descreve como seria um processo de revogação de um certificado digital usando um controle de datação. A cada troca de mensagem entre dois componentes é gravado um registro de datação. Com este dado é possível conhecer cada tarefa já realizada no processo e o tempo que levou para efetuá-la.

Para cada registro de datação que tiver a necessidade de ser incluído no certificado será definida uma extensão. Os sistemas que são compatíveis com o modelo com de controle de datação devem verificar a existência da extensão no certificado e fazer a verificação *on line*. Caso ocorra algum problema, o certificado deverá ser considerado inválido pelo sistema.

8.7 Estrutura para Armazenamento de AC-Raízes Confiáveis

Por falta de conhecimento dos usuários, não existe, atualmente, uma preocupação sobre os certificados de AC-Raízes que os navegadores trazem pré-instalados. A grande maioria dos usuários nem mesmo possuem conhecimento que eles existem.

Este desconhecimento por parte dos usuários pode acarretar em problemas, caso alguma das empresas que possui a confiança dos usuários cometa algum tipo de erro na emissão de um certificado. Recentemente, em março de 2001, uma dessas empresas emitiu dois certificados para assinatura de código para dois indivíduos que forjaram suas identidades. Por causa de características próprias, esses certificados não causaram maiores problemas, mas se os certificados emitidos fossem para outros fins, os danos

poderiam ser enormes[CAP 01].

8.7.1 Certificados de AC-Raízes Pré-Instalados

No momento que um usuário está realizando a instalação de um navegador para acessar páginas na Internet, certificados de várias AC-Raízes são automaticamente instalados e configurados como confiáveis, sem consentimento algum por parte do usuário.

Os navegadores mais conhecidos possuem muitas opções para a personalização da instalação, porém em nenhuma delas o usuário pode escolher não instalar esses certificados.

Caso alguém opte por não confiar nos certificados de alguns dos emissores que os aplicativos trazem pré-instalados, ele deverá apagar certificado por certificado da área de armazenamento do aplicativo.

O motivo pelo qual o usuário é levado a confiar nestes certificados é que a instituição responsável pela ICP foi auditada por alguma consultoria parceira da empresa desenvolvedora do navegador. A partir disso, o certificado dessa instituição é incluído na instalação do aplicativo para navegação.

Além disto o usuário deve confiar em um certificado que a empresa desenvolvedora diz ser confiável. O usuário não possui garantias que o certificado instalado em sua máquina pertence realmente àquela instituição.

Se um certificado para fins maliciosos for inserido na lista de certificados confiáveis no momento da instalação, não há maneiras do usuário provar que este certificado foi distribuído juntamente com o navegador. Isto porque não há distinção entre um certificado instalado pelo aplicativo no momento da instalação e um instalado pelo usuário posteriormente.

Também não existe preocupação alguma por parte dos desenvolvedores de assinar digitalmente a lista de certificados considerados confiáveis por eles.

8.7.2 Modelo Alternativo

Uma maneira mais segura das empresas desenvolvedoras distribuírem os certificados das AC-Raízes considerados confiáveis seria a utilização de um cartão ou dispositivo semelhante, onde estariam disponíveis todos os certificados das instituições de confiança da empresa.

Esses cartões seriam distribuídos por empresas autorizadas dos desenvolvedores. Desta maneira não seria possível que o cartão fosse forjado, assim como a lista de certificados nele disponível.

A lista de certificados incluídas no cartão deveria ser assinada digitalmente pela empresa desenvolvedora do aplicativo. Com a assinatura digital, a empresa seria responsável por qualquer certificado de origem comprovadamente errônea que seja instalado através do dispositivo por ela distribuído.

Igualmente, como todos os certificados de outras instituições, o certificado que assina a lista de certificados confiáveis não deve ser incluído no momento da instalação do aplicativo. A empresa desenvolvedora poderia sim disponibilizá-lo em sua página na Internet. Deste modo, após a instalação, o usuário pode acessar o sítio da empresa e considerá-lo confiável. Para que esta metodologia possa ser usada, a empresa desenvolvedora deve possuir um sítio seguro, garantindo a integridade das informações disponíveis em sua página. Caso contrário todo o processo está ameaçado, pois o certificado disponível pode ter sido forjado.

Além de adotar a filosofia acima, a empresa deve preocupar-se em tornar disponível para o usuário a opção de instalação de somente alguns certificados. O usuário pode querer confiar em uma instituição que possui seu certificado no cartão, mas pode não querer confiar em outras. Um processo de instalação único que inclui todos os certificados no navegador do usuário não seria a solução ideal para o problema atual, pois não teria a flexibilidade necessária.

8.8 Conclusão

Embora as ICP atuais já atendam as necessidades de segurança de algumas empresas, elas ainda podem ter características alteradas para serem utilizadas em cenários específicos.

No caso de uma ICP que deverá garantir a segurança de cidadãos e a integridade dos documentos eletrônicos de um país inteiro, cada característica deve sofrer um estudo aprofundado. Além disto, a ICP deve estar organizada de tal forma que futuras mudanças possam ser facilmente inseridas ao contexto, sem causar prejuízos para a estrutura ou para seus usuários.

Nesse capítulo foi descrito um modelo de ICP que possui uma flexibilidade muito acentuada, pois nenhuma outra estrutura estaria ligada a ele em forma descendente, ou seja, em caso de alterações elas não sofreriam um impacto direto.

Também foram sugeridas a implementação de novas características para o modelo atual, visando deixá-lo mais completo e adequando-o as características que deverão ser incrementadas às ICP em um futuro próximo.

Capítulo 9

Considerações Finais

Considerando os objetivos do trabalho foram percebidas as seguintes contribuições:

- Criação de uma base teórica que possibilitou a escrita deste trabalho, sendo ele uma excelente referência em língua portuguesa para estudos posteriores sobre Infra-estrutura de Chaves Públicas;
- Discussão sobre o modelo de Infra-estrutura de Chaves Públicas em fase de implantação pelo governo federal brasileiro;
- Indicação de um novo modelo de ICP que, através de embasamento teórico, percebeu-se atender melhor as necessidades nacionais;
- Definição de uma metodologia para disponibilização de ferramentas de código fonte aberto na Internet;
- Crítica do atual modelo de armazenamento de certificados de AC-Raízes confiáveis. Sugestão de um novo modelo que tornaria o sistema de armazenamento menos suscetível a problemas de segurança;
- Integração de uma estrutura de datação à ICP e integração de registros de datação aos certificados, impossibilitando acordos entre entidades maliciosas;
- Descentralização de parte da ICP, tornando-a menos suscetível a falhas;

- Incorporação de novos componentes à ICP com o objetivo de aumentar o número de serviços disponíveis.

A fase teórica da pesquisa foi finalizada com sucesso, propondo um modelo alternativo que possui vantagens em relação ao adotado pelo governo. Com o trabalho de pesquisa bem fundamentado, agora resta a implementação das contribuições. Abaixo serão listados alguns ítens que podem ser desenvolvidos futuramente:

- Implementação de uma entidade central do tipo Ponte;
- Desenvolvimento dos módulos que devem ser separados da Autoridade Certificadora;
- Implementação de uma estrutura contendo todos os módulos descentralizados;
- Desenvolvimento de ferramentas usando a metodologia citada na dissertação;
- Integração da Autoridade de Datação com uma Infra-estrutura de Chaves Públicas;
- Definição do protocolo da Autoridade de Aviso;
- Desenvolvimento de uma Autoridade de Aviso;

Por fim, apesar de enaltecer o trabalho sendo realizado pelo governo federal atual, procurou-se criar uma estrutura que garanta a segurança dos cidadãos e empresas que participam da chamada sociedade digital, onde muito já é realizado através de meios eletrônicos. Após uma profunda análise no modelo de segurança implementado pelo governo brasileiro, foram percebidos alguns detalhes que trazem vantagens significativas para o sistema como um todo.

Certas características do sistema atual podem desmotivar empresas a integrarem-se à ICP-Brasil. Como um reflexo disto, as mesmas podem diminuir ou até cessar seus investimentos nessa área da segurança. Sem o capital privado, as pesquisas sofreriam um grande atraso tecnológico em relação às realizadas em outros países que possuem esse aporte financeiro.

Um modelo mais flexível e adaptado às condições políticas brasileiras, utilizado em paralelo com um ferramental que garante a transparência e, principalmente, a segurança do sistema, terá uma aceitação muito maior pelos cidadãos, expandindo assim a cultura do uso de certificados digitais e garantindo uma integração segura com o mundo digital.

Referências Bibliográficas

[ADA 99] ADAMS, C.; LLOYD, S. **Understanding Public-Key Infrastructure: Concepts, Standards, and DeplymentConsiderations**. 1. ed. Macmillan Technical Publishing, 1999.

[Ada 00] **Which PKI (Public Key Infrastructure) is the Right One?** ACM Press, 2000.

[ALT 01] ALTERMAN, P. The us federal pki and the federal bridge certification authority. **Elsevier Science**, [S.l.], Dezembro, 2001.

[ARA 02] ARAÚJO, R. S. D. S. **Protocolos Criptográficos Para Votação Digital**. Florianópolis: Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[AUS 01] AUSTIM, T. **PKI - A Wiley Tech Brief**. 1. ed. Wiley Computer Publishing, 2001.

[BIC 00] BICKMORE, R. Implementing a pki. Baltimore Technologies, 2000. Relatório técnico.

[BRA] BRASIL. Lei n. 2.200-2, de 24 DE AGOSTO DE 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

[BRO 01] BROCARDO, M. L. **I2AC: Um Protocolo Criptográfico Para Análise Segura de Crédito**. Florianópolis: Universidade Federal de Santa Catarina, 2001. Dissertação de Mestrado.

[CAP 01] CAPABILITY, C. I. A. **Erroneous Verisign-Issued Digital Certificates for Microsoft**. Disponível na Internet. http://www.ciac.org/ciac/bulletins/l-062.shtml disponível em 21 abril 2002.

[CUS 01] CUSTÓDIO, R. F. Análise crítica a icp-brasil. Resposta à consulta pública sobre a regulamentação da ICP-Brasil, Novembro, 2001.

[DAN 01] DANTAS, L. A. **ECN: Protocolo Criptográfico Para Emissão de Certidão de Nascimento Na Internet**. Florianópolis: Universidade Federal de Santa Catarina, 2001. Dissertação de Mestrado.

[dC 98] DO CANADÁ, G. Government of canada public key infrastructure. Communications Security Establishment, Fevereiro, 1998. Relatório técnico.

[DER] DERENALE, C. **About EuroPKI**.

[DEV 01] DEVEGILI, A. J. **Farnel: Uma Proposta de Protocolo Criptográfico Para Votação Digital**. Florianópolis: Universidade Federal de Santa Catarina, 2001. Dissertação de Mestrado.

[EUR] EUROPKI. **Registration Authority**. Disponível na Internet. http://www.europki.org/ disponível 11 dezembro 2001.

[FEG 99] FEGHHI, J.; FEGHHI, J.; WILLIAMS, P. **Digital Certificates**. 1. ed. Addison Wesley, Setembro, 1999.

[FER 01] FERNANDES, A. D. Risking ”trust”in public key infrastructure: Old techniques of managing risk applied to new technology. **Elsevier Science**, [S.l.], p.303–322, 2001.

[FOR 01a] FORUM, W. A. P. **WPKI Wireless Application Protocol Public Key Infrastructure Definition**, 24 de abril de 2001. ed., 2001.

[FOR 01b] FORUM, W. A. P. **WTLS Wireless Transport Layer Security**, 06 de abril de 2001. ed., 2001.

[GEN 01] GENGLER, B. **Yahoo News Hacked**. Computer Fraud & Security.

[GHI 02] GHISLERI, A. S. **Sistema Seguro de Atendimento Ao Cliente: Garantia Da Qualidade de Serviço**. Florianópolis: Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[Gui 00] **Guidelines, Methodologies and Standards to set up a CA for Digital Signature**. Internet.

[HAB 91] HABER, S.; W., S. How to timestamp a digital document. **Journal of Cryptology**, [S.l.], p.99–111, 1991.

[HOU 99] HOUSLEY, R. et al. Internet x.509 public key infrastructure certificate and CRL profile. Internet Engineering Task Force, 1999. Relatório técnico.

[HOU 01] HOUSLEY, R.; POLK, T. **Planning for PKI - Best Practices Guide for Deploying Public Key Infrastructure**. 1. ed. Wiley Computer Publishing, 2001.

[HUN 00] HUNT, R. Technological infrastructure for PKI and digital certification. **Elsevier Science**, [S.l.], p.1460–1471, Dezembro, 2000.

[Jag 99] **Querying Network Directories**. ACM Press, 1999.

[LAB] LABORATORIES, R. **Public-Key Cryptography Standards**. Disponível na Internet. http://www.rsasecurity.com/rsalabs/pkcs/ disponível em 16 abril 2002.

[LAB 93] LABORATORIES, R. **PKCS #7: Cryptographic Message Syntax Standard. Version 1.5**.

[LAB 00] LABORATORIES, R. Pkcs #10 v1.7 : Certification request syntax standard. RSA Laboratories, Maio, 2000. Relatório técnico.

[MIG 02] MIGNONI, M. E. **Políticas e Declaração de Práticas de Certificação**. Florianópolis: Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[MIT 00] MITCHELL, C. Pki standards. University of London, 2000. Relatório técnico.

[NOT 02] NOTOYA, A. E. **IARSDE- Infra-Estrutura de Armazenamento e Recuperação Segura de Documentos Eletrônicos**. Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[PAS 02] PASCAL, E. S. **IDDE - Uma Infra-Estrutura Para a Datação de Documentos Eletrônicos**. Florianópolis: Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[PEA 00] PEARSON, H. E. Open source - the death of proprietary systems? **Computer Law & Security**, [S.l.], v.Volume 16, 2000.

[PRO] PROJECT, G. **Open Source**. Disponível na Internet. 11 dezembro 2001.

[RES 01] RESCORLA, E. **SSL and TLS Designing and Building Secure Systems**. Primeira. ed. Addison-Wesley, 2001.

[ROC 01] ROCHA, J. L. F. **Proteção de Software Por Certificação Digital**. Florianópolis: Universidade Federal de Santa Catarina, 2001. Dissertação de Mestrado.

[SCH 96] SCHNEIER, B. **Applied Cryptography - Protocols Algorithms, and Source Code in C**. Segunda. ed. John Wiley & Sons, Inc, 1996.

[SCH 02] SCHEFFEL, G. V. **Segurança Na Avaliação Não Presencial**. Florianópolis: Universidade Federal de Santa Catarina, 2002. Dissertação de Mestrado.

[SEC 00] SECURITY, N. **IBM to adopt open source**.

[STA 99] STALLINGS, W. **Cryptography and Network Security - Principles and Practice**. 2. ed. Prentice-Hall, 1999.

[STI 95] STINSON, D. R. **Cryptography - Theory and Practice**. 1. ed. CRC Press LLC, 1995.

[UNI 97] UNION, I. T. **ITU-T Recommendation X.509**.

[Woh 00] **Digital Certificates: A Survey of Revocation Methods**. ACM Press, Novembro, 2000.

[WRI 99] WRIGHT, M. A. An overview of pki. **Network Security**, [S.l.], Setembro, 1999.

Glossário

Aplicativo Compilado - Aplicativo em modo binário onde somente sua execução é possível.

Assinante - Indivíduo que cifra algo com sua chave privada, obtendo como resultado uma assinatura digital.

Ator - nome dado ao indivíduo, máquina ou mecanismo envolvidos em uma transação eletrônica.

Chave de cifragem - Chave simétrica criada para ser utilizada em uma única operação de cifragem. Esta chave é cifrada usando o par de chaves assimétricas.

Chave Privada - Chave de criptografia que deve ser mantida em sigilo.

Chave Pública - Chave de criptografia de conhecimento público.

Encapsulamento - Inserção de uma mensagem dentro de outra.

Função Resumo - Função matemática efetuada em um conjunto de caracteres de tamanho variável gerando um resultado de tamanho fixo.

Mensagem envelopada - Mensagem contendo o Texto Cifrado.

Texto Aberto - Texto legível para qualquer pessoa.

Texto Fechado ou Cifrado - Resultado do texto depois do processo de criptografia. Legível somente para determinados usuários.

X.509 - Recomendação do ITU-T para o formato de certificados digitais.