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

Marcelo Carlomagno Carlos

Topologias dinâmicas de Infra-estrutura de Chaves Públicas

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

Florianópolis, Agosto de 2007

Topologias dinâmicas de Infra-estrutura de Chaves Públicas

Marcelo Carlomagno Carlos

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

Rogério Cid Bastos, Dr.
Coordenador do Curso

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Joni da Silva Fraga, Dr.

Luiz Carlos Zancanella, Dr.

Frank Augusto Siqueira, Dr.

"A morte do homem começa no instante em que ele desiste de aprender"

Albino Teixeira

À minha família que tornou a realização deste trabalho possível.

Agradecimentos

Primeiramente agradeço ao meu orientador, o professor Ricardo Felipe Custódio, por campartilhar de seu conhecimento acadêmico, didático e de vida, além de mostrar-se um grande amigo.

Aos professores Frank Augusto Siqueira, Joni da Silva Fraga e Luiz Carlos Zancanella pelas importantes contribuições.

Aos meus familiares, a quem devo grande parte de tudo o que conquistei e conquistarei durante minha vida, especialmente aos meus pais Hélio Aparecido Carlos e Maria Teresa Carlomagno Carlos.

À minha namorada Vania, por seu companheirismo, amor, amizade, compreensão e principalmente incentivo, sem o qual não seria possível a realização deste trabalho.

Ao Jeandré Monteiro Sutil, que muito contribuiu com inúmeras conversas e trocas de idéias que vieram a compor o conteúdo aqui apresentado.

Aos membros do LabSEC pelas discussões diárias sobre os mais diversos assuntos que certamente me ajudaram a chegar até este momento.

A todos os meus amigos que sempre me apoiaram e estiveram ao meu lado durante esta jornada.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

AC	Autoridade Certificadora
ACU	Autoridade Certificadora Única
AR	Autoridade de Registro
CTL	Certificate Trust List
CMP	Certificate Management Protocol
DPC	Declaração de Práticas de Certificação
ICP	Infra-Estrutura de Chaves Públicas
ISO	International Standards Organization (Organização Internacional de Padrões)
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector
LCR	Lista de Certificados Revogados
PC	Política de Certificação
PKCS	Public-Key Cryptography Standards
RFC	Request For Comments
RSA	Rivest, Shamir e Adelman

Resumo

Esta dissertação de mestrado contém propostas para que a gerência do ciclo de vida de uma Infra-estrutura de Chaves Públicas seja tratada dinamicamente, tornando possível a substituição eficiente de certificados e chaves criptográficas de suas entidades, sem comprometer a topologia como um todo. As técnicas e métodos previstos na literatura são eficientes mas existem situações nas quais estas técnicas não possuem a abrangência necessária para solucionar determinados problemas. Devido a isso, foi realizada uma nova classificação para a separação entre as possíveis operações de substituição de chaves e certificados, e para os casos não previstos, foram propostos novos métodos e procedimentos. A partir dos resultados obtidos, são apresentadas novas aplicações práticas derivadas destas técnicas com a finalidade de torná-las ainda mais dinâmicas e atender as demandas de aplicações reais. Na parte final deste trabalho, são apresentados os mecanismos de testes e validação aplicados sobre estas propostas, de forma a mostrar sua eficácia e integração com as principais aplicações práticas atualmente em uso.

Palavras Chaves: Infra-Estrutura de Chaves Públicas, ICP dinâmica, Topologias de ICP, Gerenciamento de ICP

Abstract

This masters dissertation contains proposals for dynamic treatment of Public Key Infrastructure life cycle management, making possible the efficient replacement of its certificates and cryptographic keys without compromising the whole topology. The techniques and methods that exists in the literature are efficient, however there are some cases which these techniques are not enough to solve some problems. Thus, a new classification for the certificates and keys replacement operations have been created, and to the not foreseen cases, new methods and procedures had been proposed. With the acquired results, new practical applications have been derived aiming at making them more dynamic and assist demands of real applications. At the end of this work, tests and validation mechanisms that was applied are presented, showing its efficiency and integration with the main applications in use today.

Keywords: Public Key Infrastructure, Dynamic PKI, PKI topology, PKI management

Capítulo 1

Introdução

O uso em larga escala de chaves públicas para propiciar segurança às comunicações e transações eletrônicas em computadores só foi possível graças à estruturação de mecanismos criptográficos e de técnicas de gestão na forma de uma infra-estrutura de chaves públicas (ICP) e ao esforço da comunidade científica e de organizações empresariais na elaboração de normas e recomendações [1, 2] que regulamentam a forma adequada de se implementar uma ICP. Entretanto, constatou-se após duas décadas de uso, que estas normas são extremamente rígidas e não prevêem determinadas funcionalidades as quais dificultam a operação a longo prazo da ICP. Um desses problemas, o qual este trabalho trata, consiste na substituição do certificado ou do par de chaves criptográficas de Autoridades Certificadoras (AC).

As recomendações RFC 3280 [1] e RFC 4210 [2] prevêem apenas um caso para a substituição do par de chaves de uma AC. Este se refere à substituição das chaves quando o antigo par de chaves da AC está disponível. Entretanto, à medida que os certificados digitais de AC reais começaram a expirar, surgiram situações não previstas nestas normas. São os casos quando não se tem acesso à chave privada anterior da AC ou quando não se pode realizar, por restrições do hardware, do protocolo de gestão de chaves ou da política, a cópia da chave privada antiga. Não há referências na literatura especializada de mecanismos para tratar adequadamente estes problemas.

1.1 Objetivos

O objetivo deste trabalho é apresentar mecanismos que possibilitem o processo de gerência de ICPs a longo prazo, descrevendo os procedimentos necessários para a substituição de chaves ou certificados de Autoridades Certificadoras.

1.1.1 Objetivos específicos

Este trabalho possui os seguintes objetivos específicos:

- Apresentar mecanismos para a troca do par de chaves de uma AC;
- Apresentar mecanismos para a substituição do certificado de uma AC;
- Apresentar mecanismos para tratar a perda da chave privada de uma AC;
- Descrever o impacto dos modelos discutidos sobre a topologia da ICP;
- Apresentar novos métodos para aumentar o dinamisco das ACs;
- Discutir e apresentar o comportamento de ferramentas atuais após a aplicação dos modelos.

1.2 Justificativa e Motivação

A presente dissertação de mestrado é um dos frutos do programa João de Barro, que tem como objetivo a substituição da plataforma criptográfica da Autoridade Certificadora Raiz Brasileira (ICP Brasil). O programa João de Barro é capitaneado pelo Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal vinculada à Casa Civil da Presidência da República, criada pela Medida Provisória (MP) número 2.200-2, de 24 de agosto de 2001 [3]. Nesta MP, o ITI é designado como a AC Raiz brasileira. A resolução número 20 do Comitê Gestor da ICP Brasil, de 08 de maio de 2003, determina à AC Raiz, o desenvolvimento de uma plataforma aberta (hardware e software) voltada à execução das funções criptográficas da AC Raiz da ICP-Brasil, com a garantia da auditagem plena desta plataforma e dos sistemas embarcados presentes nos hardwares [4].

Esta resolução foi motivada pelo fato de que a atual plataforma, de origem estrangeira, utiliza software proprietário, o que tem dificultado sua auditoria e confiabilidade [5, 6]. Após a implementação da nova plataforma, esta deverá ser colocada em operação em substituição à plataforma atualmente em uso. Sabe-se, contudo, que tal substuição não pode ser realizada de forma simples, e deve ser estabelecido um ritual detalhado do processo, com previsão de todos os impactos que tal substuição provocará na árvore de certificação da ICP-Brasil.

Entre os problemas que devem ser estudados e propostas soluções, há a questão de como substituir de forma eficaz e segura o par de chaves criptográficas e o certificado da AC Raiz. Assim, a motivação deste trabalho foi o estudo e criação de técnicas eficientes que facilitem a substituição da AC Raiz Brasileira atualmente em uso por uma nova AC Raiz gerando o menor impacto possível sobre sua topologia e ACs credenciadas. No entanto, os resultados deste trabalho não se destinam unicamente ao escopo da ICP Brasil, sendo aplicáveis a quaisquer outras ICPs.

1.3 Metodologia

Para se alcançar os objetivos deste trabalho, foram estudados diversos artigos, normas e publicações cujo tema fosse relacionado a gerência de Infra-estrutura de chaves Públicas, substituição de chaves criptográficas e certificados de Autoridades Certificadoras e construção de caminho de certificação.

As avaliações de cada trabalho estudado foram realizadas analisando a abrangência e as necessidades de cada um deles. Com isto, foi realizado o mapeamento de todas as possíveis ações de substituição de certificados e chaves criptográficas de Autoridades Certificadoras.

Após esta análise, foram estudadas e implementadas formas de suprir as carências encontradas, principalmente a ausência de métodos que tratem o comprometimento da chave privada de uma Autoridade Certificadora. Na seqüência, foi definida uma abordagem centrada nas possíveis operações de substituição de certificados e chaves. Com isto, foi possível estabelecer uma maior abrangência e estabelcer procedimentos que causem menor impacto sobre a ICP neste processos de substituição. Por fim, foram implementados protótipos para testes e validação das propostas além da verificação de suas

aplicabilidades em ambientes reais.

1.4 Limitações do trabalho

No presente trabalho não serão abordados aspectos relativos ao processo de criação do par de chaves, e dos critérios de verificação de restrições de segurança das chaves privadas.

Embora existam outros modelos de infra-estruturas de chaves públicas (ICP) e certificados digitais, tais como o SPKI [7] e o PGP [8], o escopo deste trabalho se restringe apenas ao padrão X.509.

Este trabalho não trata diretamente das implicações da aplicação dos métodos descritos sobre os documentos de Políticas de Certificação (PC) e Declaração de Práticas de Certificação (DPC) de uma ICP.

Adicionalmente, nenhum aspecto de caráter privativo da ICP Brasil e do programa João de Barro é tratado neste documento. Em virtude disso, este trabalho não escolhe a melhor solução para a substituiçao das chaves e certificados da ICP Brasil e sim, serve como insumo teórico-científico de todas as possibilidades, as quais podem ser levadas em consideração pelos gestores para tal substituição.

1.5 Estrutura do Trabalho

No capítulo 3 são detalhadas informações relevantes sobre Infra-estrutura de Chaves Públicas para que posteriormente sejam apresentadas as diferentes formas e necessidades das ICPs. No capítulo 4 são apresentados os métodos de substituição de chaves e certificados de ACs existentes atualmente nas recomendações e artigos publicados. Prosseguindo, no capítulo 5, se encerra a revisão da literatura e se iniciam as principais contribuições deste trabalho, onde são descritas as falhas dos modelos atuais e é apresentada uma análise de todos os tipos possíveis de trocas de chaves e certificados, e um respectivo método para a realização de cada um deles. No capítulo 6 são apresentados métodos de modificação dinâmica de topologias de ICPs derivados dos modelos apresentados anteriormente. Na seqüência, no capítulo 7 são apresentados os procedimentos de testes e validação realizados e seus respectivos resultados. Por fim, as considerações

finais advindas da pesquisa deste trabalho são apresentadas no capítulo 8.

Capítulo 2

Fundamentos de Criptografia

O objetivo principal da criptografia é permitir que duas pessoas/partes possam se comunicar através de um meio inseguro de forma que uma terceira pessoa não consiga entender o conteúdo que está sendo transmitido [9]. A partir da utilização de criptografia pode-se prover os seguintes serviços [10]:

Autenticação - busca garantir que a comunicação é autêntica, ou seja, que as entidades envolvidas são quem clamam ser.

Controle de Acesso - é a habilidade de limitar e controlar o acesso a sistemas e aplicações.

Confidencialidade - garante o sigilo da mensagem, evitando que seu conteúdo ou informações sobre o conteúdo sejam visualizadas em uma tentativa de ataque.

Integridade - permite a verificar se a mensagem enviada é a mesma mensagem que foi recebida ou se sofreu alguma alteração.

Não repúdio - previne que o emissor ou receptor neguem a autoria de uma mensagem.

2.1 Criptografia Simétrica

A criptografia simétrica tem como principal característica o uso da mesma chave criptográfica para cifrar e decifrar informações. Desta forma, uma mesma chave é compartilhada pelo emissor e receptor para que a confidencialidade no tráfego de informações seja garantida.

Como se pode observar na figura 2.1, quando Alice deseja enviar uma mensagem sigilosa para Beto, ela escolhe um algoritmo simétrica e uma chave criptográfica que Beto conheça. Alice cifra o conteúdo da mensagem utilizando o algoritmo e a chave escolhida transformando a mensagem em texto cifrado. Beto, ao receber o texto cifrado, utiliza a chave que compartilha com Alice e através do algoritmo de decifragem, transforma o conteúdo cifrado novamente em texto plano. Se alguma entidade interceptar o conteúdo da mensagem durante o envio de Alice para Beto, esta entidade terá acesso apenas ao texto cifrado e por não conhecer a chave compartilhada por Alice e Beto, não terá acesso ao conteúdo da mensagem, restando apenas a tentativa de um ataque de força bruta, ou seja, tentar todos os possíveis valores de chaves. Algo que se pode notar neste caso é que o modo de distribuição das chaves entre Alice o Beto é de fundamental importância para garantir a segurança no processo.

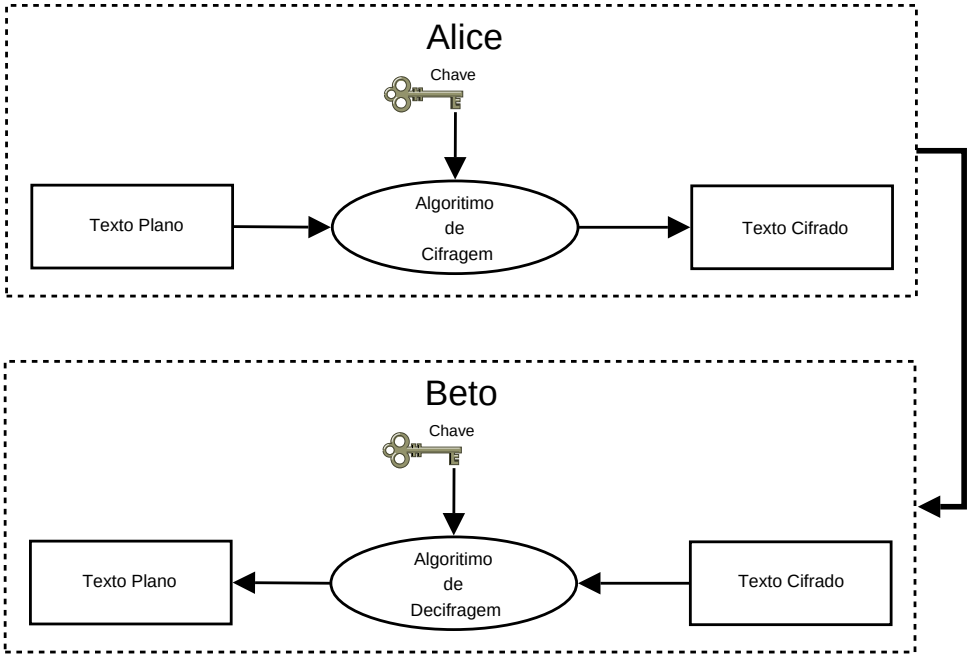

Figura 2.1: Processo de cifragem e decifragem simétrica

Dentre os algoritmos de criptografia simétrica atuais, merecem destaque o *Data Encryption Standard* (DES) [11] e seu substituto, o *Advanced Encryption Standard* (AES) [12].

2.2 Criptografia Assimétrica

A criptografia assimétrica, também chamada de criptografia de chave pública foi inicialmente proposta por Diffie e Hellman em 1976 [13] e tem como base a utilização de duas chaves distintas, uma privada (KR) e uma que pode ser mantida pública (KU). Embora sejam complementares, o valor da chave privada não pode ser extraído a partir da chave pública. Para cifrar e decifrar informações, a criptografia assimétrica se dá de forma complementar, onde tudo o que é cifrado com a chave pública só é decifrado com sua respectiva chave privada.

Este paradigma simplifica o gerenciamento do uso de chaves simétricas para cifragem, reduzindo significativamente o número de chaves a serem armazenadas por longos períodos. Esta redução se dá pelo fato de que as chaves simétricas são utilizadas por um curto período de tempo e depois descartadas. Apenas a chave privada precisa ser protegida por um longo período de tempo [14]. Outra vantagem deste paradigma é que com a possibilidade de livre distribuição de chaves públicas, entidades que não se conhecem podem trocas mensagens sigilosas.

Baseado nas idéias de Diffie e Hellman, o algoritmo desenvolvido por Ron Rivest, Adi Shamir e Len Adleman, o RSA, surgiu em 1977 e até hoje é o algoritmo mais utilizado e aceito na cifragem de dados utilizando criptografia de chaves públicas [15, 16]. 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 pode ser utilizado apenas para assinatura digital, não podendo ser utilizado para cifragem e distribuição de chaves [17].

2.3 Funções Resumo

Funções de resumo criptográfico recebem entradas de tamanho qualquer e produzem uma saída de tamanho fixo. Elas têm grande utilidade quando se trata de segurança pelo fato de ser um eficiente meio de detectar corrompimento de dados. Uma vez que foi gerado o resumo criptográfico de um conjunto de dados, se os dados originais forem modificados, o resultado de uma nova aplicação da função possuirá uma saída diferente do resultado sobre os dados originais [18]. O Objetivo de uma função de resumo

criptográfico é produzir uma impressão digital de um conjunto de dados [9].

Diferentemente dos processos de cifragem e decifragem de dados, as funções resumo são funções de sentido único, ou seja, uma vez obtido o resumo criptográfico, não é possível obter a mensagem original a partir de seu conteúdo. Outra característica relevante deste tipo de função é que basta alterar um bit de uma mensagem e o resumo produzido será completamente diferente.

O tamanho gerado pela saída de uma função de resumo criptográfico varia de acordo com o algoritmo utilizado. Entre os algoritmos mais conhecidos e utilizados atualmente estão o MD5 [19] e SHA1 [20].

2.4 Assinatura Digital

Uma assinatura digital consiste em um conjunto de dados em forma eletrônica que atestam que o assinante conhece o conteúdo do documento eletrônico assinado. O processo de assinatura consiste em cifrar o resumo criptográfico de um documento eletrônico com a chave privada do assinante. Já para a verificação de uma assinatura digital, é necessário decifrar a assinatura gerada com a chave pública do assinante e comparar o resultado dessa operação com o resumo do documento original. A figura 2.2 representa este processo.

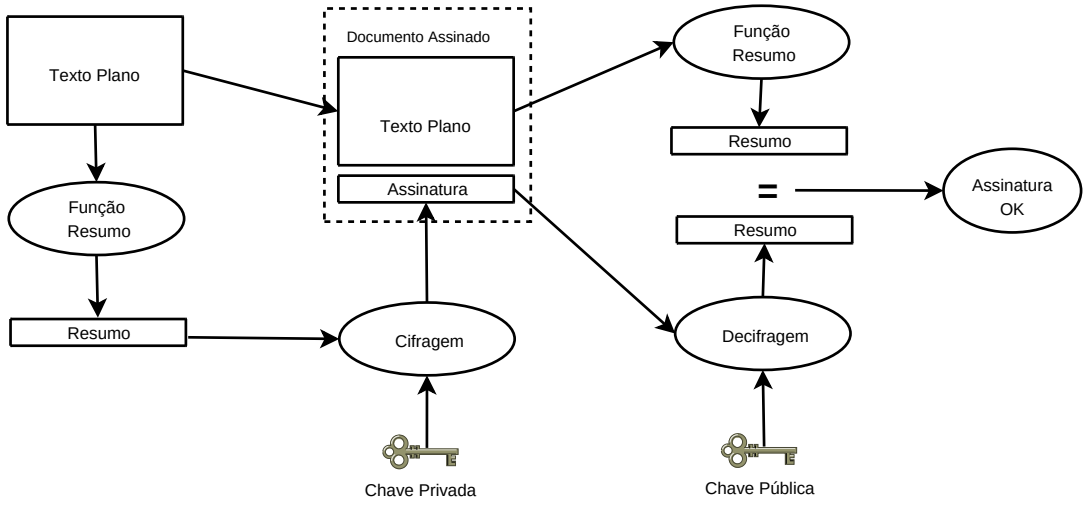

Figura 2.2: Processo de assinatura de um documento eletrônico e sua respectiva verificação

A autenticação da chave pública é um requisito necessário para que quem verifica a assinatura saiba que a chave pública utilizada neste processo corresponda

à chave privada pertencente somente ao assinante. Caso contrário, embora seja possível verificar a integridade da mensagem, não haverá forma de saber quem assinou o documento. Para relacionar uma chave pública ao usuário que possui a chave privada surgiram os certificados digitais, que buscam dar identidade a uma chave pública [14].

Capítulo 3

Infra-estrutura de Chaves Públicas

Com o advento da criptografia de chaves públicas e o conceito da existência de uma chave pública que pode ser distribuída livremente, surgiram novas necessidades e questões a serem tratadas. Entre elas, merece destaque a questão de como associar uma chave pública a seu responsável.

Loren Kohnfelder [21] introduziu o conceito de utilização de uma entidade confiável para atestar a ligação entre uma entidade e sua respectiva chave pública, dando origem aos certificados digitais e à idéia de uma entidade que posteriormente seria chamada de Autoridade Certificadora (AC).

A AC é a entidade responsável pela identificação do usuário e por atestar que ele possui a chave privada correspondente à chave pública. Este processo é realizado através da assinatura de um documento pela AC que contém dados de identificação do usuário, sua chave pública e outros atributos necessários. Este documento é chamado de Certificado Digital e representa o mais básico elemento de uma Infra-estrutura de Chaves Públicas (ICP).

3.1 Certificados Digitais de Chaves Públicas

Um dos principais problemas da criptografia de chaves públicas é determinar quem possui a chave privada correspondente. Para solucionar este problema, foi proposto o uso de Certificados Digitais de Chaves Públicas, ou simplesmente certificados. Cada certificado contém a chave pública e a identificação da entidade que controla a respectiva chave privada [14].

Segundo Housley [14], um certificado ideal deve conter uma série de características importantes:

a) deve ser um objeto puramente digital, para que possamos distribuí-lo via internet e processá-lo automaticamente;

b) deve conter o nome do usuário que detém a chave privada, além da empresa ou organização a qual pertence e informações de contato;

c) deve ser fácil de determinar se o certificado foi recentemente emitido;

d) deve ser criado por uma entidade confiável ao invés do próprio usuário que detém a chave privada;

e) uma vez que uma entidade confiável pode criar vários certificados, inclusive para um mesmo usuário, deve ser fácil diferenciá-los;

f) deve ser fácil determinar se o certificado foi forjado ou se é genuíno;

g) deve ser à prova de violação de modo que ninguém consiga alterá-lo;

h) deve ser possível verificar de forma imediata se alguma informação no certificado não é mais válida;

i) deve-se poder determinar para quais aplicações o certificado é válido.

O certificado digital de chaves públicas, como especificado pelo ITU-T [22], trata-se um objeto puramente digital que contém informações sobre o proprietário da chave a ele relacionada, tais como nome, empresa onde trabalha, informações para contato, etc. Além disso, possui dois campos de data indicando sua data de emissão e de expiração, informações sobre a entidade que emitiu o certificado e uma assinatura digital realizada por seu emissor, o que garante a característica de ser à prova de modificação.

Após passar por duas revisões [23, 24], ficaram claras algumas necessidades dos certificados de chaves públicas, sendo a mais importante a necessidade de carregar um maior número de informações. Com isso, em junho de 1997 os certificados digitais de chaves públicas ganharam uma nova característica, conhecida como extensões, e juntamente à sua especificação, foram criadas algumas extensões pré-definidas

para prover informações adicionais à identificação da entidade, tais como atributos da chave e restrições do caminho de certificação.

As duas últimas propriedades listadas não podem ser diretamente providas pelo certificado digital de chaves públicas, o que torna necessária a inserção de mecanismos adicionais para a sua obtenção: as listas de certificados revogados e as políticas de certificados que serão descritas nas seções 3.2 e 3.3 respectivamente.

3.2 Listas de Certificados Revogados

As informações contidas em um certificado digital podem ter a necessidade de serem atualizadas antes do término de seu período de validade. Porém, por se tratar de um objeto digital e de fácil difusão, é praticamente impossível notificar a todos a mudança ou recuperar e destruir todas as cópias dos certificados distribuídos. Além da atualização de dados, vários outros motivos podem gerar a necessidade de revogação de um certificado, como o comprometimento da chave privada, cancelamento do uso do certificado, comprometimento da chave privada da Autoridade Certificadora, etc.

Para revogar os certificados digitais são utilizadas as listas de certificados revogados (LCR) [1], que são listas emitidas periodicamente por uma Autoridade Certificadora ou uma entidade à qual foi delegada esta função, que contém a relação dos certificados que não são mais válidos.

Uma LCR é um objeto digital, o que permite a distribuição, processamento e validação de forma eletrônica, de maneira semelhante a um certificado. A LCR é assinada pela entidade que a emitiu, permitindo a verificação de sua integridade, e possui dois campos de data, um com a data de sua emissão e outra com a data de expiração, a lista dos números seriais dos certificados emitidos, a data da revogação do certificado e extensões (opcional).

Cada LCR tem um escopo particular. O escopo é o conjunto de certificados que podem aparecer na LCR. Por exemplo, "todos os certificados emitidos pela AC A", "Todos os certificados emitidos pela AC X revogados por comprometimento de chave privada", etc [1]

Uma LCR lista todos os certificados não expirados, em seu escopo, que foram revogados por uma das razões cobertas por seu escopo. Uma LCR também pode

gerar delta LCRs, que lista apenas os certificados cujo status de revogação foi alterado desde a emissão da LCR completa de referência (LCR base). O escopo de uma delta LCR deve ser o mesmo da LCR que ela referencia.

3.3 Políticas de Certificação

As políticas de emissão de certificados são documentos escritos pelos responsáveis de uma Autoridade Certificadora, e constituem a base para auditoria, delegação de autoridade ou qualquer outra necessidade da AC. Normalmente são criados dois documentos, as Políticas de Certificação e as Declarações de Práticas de Certificação (DPC).

As políticas de certificação vêm para preencher a necessidade de se definir o propósito do certificado digital, ou seja, o seu uso. O padrão X.509 [24] define Política de Certificação (PC) como "um conjunto de regras que indicam a aplicabilidade de um certificado a uma comunidade e/ou classe de aplicação em particular de aplicações com requisitos de segurança em comum".

As DPCs são um conjunto de práticas que uma AC emprega na emissão de certificados. Uma DPC estabelece práticas relevantes ao ciclo de vida do certificado, tais como sua emissão e gerenciamento. [25]

De maneira geral, as PCs são documentos de mais alto nível sobre os requisitos e restrições associados com o uso dos certificados sob esta política, enquanto as DPCs são extremamente detalhadas e descrevem os procedimentos internos de operação da AC ou de toda uma ICP.

3.4 Componentes de uma ICP

Uma infra-estrutura de chaves públicas envolve inúmeras tarefas com diferentes níveis de relevância de acordo com as necessidades da ICP. Tarefas como gerenciamento dos certificados emitidos, emissão de listas de certificados revogados, verificação dos dados das requisições de certificados entre outras, podem exigir de uma ou mais entidades para a melhor gerência de toda a ICP.

Nesta seção serão descritos os possíveis componentes de uma ICP para

que seja possível uma melhor compreensão da importância e do uso de cada um deles.

3.4.1 Autoridades Certificadoras

A Autoridade Certificadora (AC) é uma composição de *hardware*, *software* e pessoas que a operam. Trata-se do elemento de uma ICP, responsável pela emissão de certificados, emissão de LCRs, gerenciamento e publicação das informações sobre certificados revogados além de ser capaz de delegar determinadas funções à outras entidades.

Quando uma AC emite um certificado, ela assegura que a entidade requisitante detém à chave privada correspondente a chave pública contida em seu conteúdo. Desta forma, ao assinar o certificado, a AC garante a autenticidade e validade do conteúdo do certificado, e opcionalmente inclui informações que foram consideradas relevantes. Os certificados emitidos podem ser para outras ACs, para entidades finais ou ambos.

Ao emitir LCRs, uma AC gera uma lista assinada contendo informações sobre os certificados revogados, tais como a data e o motivo da revogação. De maneira semelhante ao certificado, quando uma AC assina sua LCR, ela atesta seu conhecimento e a autenticidade do conteúdo da lista.

Uma infra-estrutura de chaves públicas pode ser constituída por uma única AC, porém em muitos casos faz-se necessário que determinadas tarefas sejam delegadas a outras entidades a fim de minimizar a carga de tarefas sobre a AC. Por exemplo, uma AC pode delegar à outra AC, denominada AC intermediária, emitir certificados em seu nome, ou então delegar a emissão da LCR a outra AC. Outra delegação de tarefa bastante comum em uma AC é de delegar o processo de identificação dos usuários para uma entidade chamada Autoridade de Registro (AR), que será descrita com maiores detalhes na seção 3.4.2.

3.4.2 Autoridades de Registro

A Autoridade de Registro (AR) é uma entidade composta por *software*, *hardware* e operadores para qual a AC delega a tarefa de verificar o conteúdo de requisições de certificados. Através da assinatura da AR, uma AC pode ter certeza que os dados recebidos foram verificados pela AR de sua confiança.

Uma AC pode delegar a tarefa de verificação de informações para várias ARs, as quais podem desempenhar seu papel para várias ACs.

A existência desta entidade em uma ICP faz-se necessária de acordo com a abrangência que uma AC pode ter, seja ela por sua distribuição geográfica, ou por um elevado número de usuários. Outro motivo para a criação de ARs pode ser a necessidade de emissão de diferentes tipos de certificados, o que pode exigir diferentes maneiras de verificação dos dados.

3.4.3 Repositório de Certificados

O Repositório de Certificados Digitais também atua por delegação da AC, e é normalmente composto por software com o objetivo de publicar os certificados digitais e listas de certificados revogados atuais emitidos por uma ou mais ACs.

A existência do repositório de certificados digitais se dá pela necessidade de interação da AC e seus usuários, e também a obtenção dos certificados e das LCRs.

Os dados disponibilizados e armazenados pelo Repositório de Certificados Digitais são assinados pela AC representada por ele, garantindo sua integridade e sua autenticidade e tornando-o imune a ataques de substituição e fabricação [14].

Diferentemente das ACs e das ARs, o Repositório de Certificados Digitais é uma parte da ICP que necessita estar sempre disponível, e por isso, necessitam de medidas de segurança. A partir da delegação desta tarefa por parte da AC, é possível que ela consiga um maior grau de proteção para sua chave privada, pelo fato de não se comunicar com qualquer outro computador.

3.4.4 Arquivo de Certificados Digitais

Semelhante à AR e ao Repositório de Certificados Digitais, o Arquivo de Certificados Digitais também atua por delegação das ACs, e é composto de software e hardware utilizados para armazenar certificados digitais e listas de certificados revogados emitidos por uma AC após o seu período de validade.

O Arquivo de Certificados Digitais pode manter por prazo indeterminado os certificados digitais emitidos pela AC, para que estas informações possam ser utilizadas na validação e verificação de antigos documentos assinados digitalmente [14]. Em geral normas jurídicas definem o tempo de armazenamento dos documentos.

3.4.5 Módulo Público

O Módulo Público fornece uma interface para que uma entidade que deseje um certificado possa fazer a solicitação. A importância do módulo público se dá pelo fato de não haver necessidade da entidade requisitante ter acesso direto a uma AR ou uma AC, reforçando a proteção sobre a chave privada da AC.

No Módulo Público podem ser encontrados também as LCRs e os certificados digitais de uma AC. Isto supre as necessidades do usuário que necessita dessas informações, sem que ele tenha o acesso direto à AC. Uma única Autoridade Certificadora pode conter vários módulos públicos.

3.4.6 Entidades Finais

Uma Entidade Final é um objeto qualquer, detentor de um certificado digital, e que não possui permissão de assinar novos certificados digitais. Objeto pode ser uma pessoa, uma aplicação, dispositivo, etc.

As entidades finais são peças importantíssimas de todo o mecanismo de uma ICP, pois todo esse processo de certificação estabelecido e toda a estrutura criada são voltados para a emissão dos certificados de entidades finais. Podem ser divididos em duas classes [14]:

- Detentores de certificados – são usuários que possuem um certificado emitido a partir de uma ICP, e utilizam sua chave privada para assinaturas, cifragem de dados e trocas de chave de sessão;
- Entidades que confiam no certificado – são usuários que utilizam certificados de outras entidades para implementar serviços em segurança, tais como verificação de assinaturas, cifragem de dados, e estabelecimento de conexões seguras, etc.

Quando usamos certificados emitidos em uma ICP, é bastante comum que se atue alternadamente entre estas duas classes.

3.5 Arquiteturas de ICP

As infra-estruturas de chaves públicas, além de prover as características definidas no decorrer deste capítulo, também precisam ser escaláveis para que uma en-

tidade possa identificar e definir se confia não em certificados emitidos por outras ACs. Além disso, é necessário que se defina de que maneira esta confiança deve ser estabelecida.

As arquiteturas de ICPs surgem a partir desta necessidade e descrevem a organização de suas ACs e relações de confiança. Cada arquitetura possui diferentes aplicabilidades, além de vantagens e desvantagens de acordo com seu formato. No decorrer desta seção, serão apresentadas 7 arquiteturas que podem ser agrupadas em três diferentes grupos de acordo com suas aplicabilidades [14]:

Arquiteturas Simples – são arquiteturas utilizadas em pequenos ambientes, pequenas empresas, dentre as quais se destacam a AC Única e as Listas de Confiança.

Arquiteturas Organizacionais – são comumente aplicadas em grandes organizações ou agências governamentais, dentre as quais se destacam as estruturas Hierárquica e em malha;

Arquiteturas Híbridas – são comumente aplicadas em grandes organizações e ambientes distribuídos, dentre as quais se destacam as Listas Estendidas de Confiança, a Certificação Cruzada e a Certificação em Ponte.

3.5.1 AC Única

A AC Única trata-se da mais simples arquitetura de ICP existente, onde uma única Autoridade Certificadora é implementada, e esta é responsável por toda a gerência e controle de uma ICP. Operações como emissão de certificados digitais, emissão de listas de certificados revogados e o controle sobre essas informações são de total responsabilidade da AC Única. A Figura 3.1 ilustra esta arquitetura. As setas representam certificados, os círculos preenchidos representam Autoridades Certificadoras, enquanto os outros círculos representam entidades finais.

Neste modelo, para que se estabeleça confiança entre os usuários, basta que estes confiem apenas em certificados e LCRs emitidos pela AC que emitiu seu próprio certificado, sem necessidade de estabelecimento de confiança em outras ACs. [14]

Por exemplo, para que Alice confie no certificado digital de Beto basta que o certificado digital dele tenha sido emitido pela mesma AC de Alice. Como con-

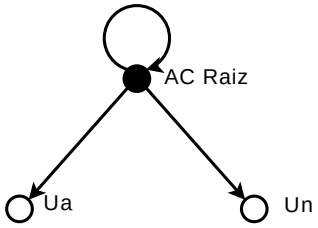

Figura 3.1: Arquitetura de ICP baseada em AC única.

seqüência disso, a construção e validação do caminho de certificação pode ser realizada a partir da posse de apenas um certificado de AC e de uma LCR.

Embora extremamente simples quando se trata de uso, implementação e validação, esta arquitetura apresenta duas limitações que devem ser analisadas. A primeira é que o modelo AC Única se torna inviável de se utilizar em grandes organizações, quando se faz necessário o estabelecimento de confiança entre duas ou mais organizações [26]. A segunda limitação, e a de maior impacto sobre a ICP, ocorre quando a AC é comprometida. Neste caso é necessário que todos os usuários pertencentes à ICP sejam notificados e além disso seja criado um novo par de chaves e um novo certificado para a Autoridade Certificadora, e reemitidos todos os certificados pertencentes a esta ICP.

3.5.2 Listas de Confiança

Trata-se de uma evolução da arquitetura de AC Única para solucionar a limitação de escalabilidade das ACs Únicas. As listas de confiança permitem que usuários de diferentes ACs possam estabelecer relações de confiança entre si. É importante ressaltar que neste modelo não existe relação de confiança entre as ACs, e sim cada usuário possui sua própria lista de confiança. Para cada certificado de AC que um determinado usuário possui em sua lista, este automaticamente passa a confiar nos certificados emitidos por estas ACs. Por exemplo, se Alice tem seu certificado emitido por uma AC 1 e deseja estabelecer uma relação de confiança com Beto, que tem seu certificado emitido pela AC 2, basta que ela adicione o certificado da AC 2 em sua lista de confiança. A Figura 3.2 representa a arquitetura de listas de confiança.

A construção e validação do caminho de certificação no caso das listas de confiança é semelhante à realizada na arquitetura de AC Única, onde existe apenas a necessidade de verificar um certificado e uma LCR para cada usuário. O único incremento

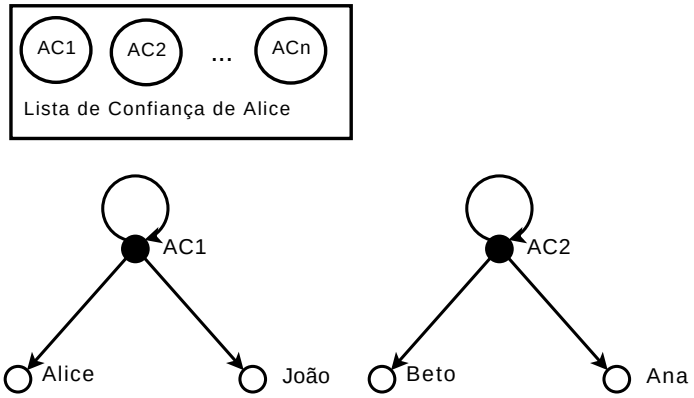

Figura 3.2: Exemplo de arquitetura de ICP baseada em Listas de Confiança.

em relação ao modelo de AC Única é a necessidade de verificar se a AC que emitiu o certificado a ser validado está na lista de confiança.

Apesar das facilidades adicionadas pelas Listas de Confiança em relação ao modelo de AC Única, as desvantagens também se tornaram maiores. O principal motivo deste aumento de desvantagens se dá pelo fato da AC não possuir nenhum controle sobre quem confia nela, e conseqüentemente aumentando a dificuldade da distribuição de informações. No caso de comprometimento de chaves, a AC não poderá informar a todos que nela confiam, tornando estes usuários vulneráveis até que a informação de revogação chegue até eles. Outra dificuldade se dá pelo fato do usuário ter que gerenciar e verificar informações sobre várias ACs simultaneamente, e conforme a lista vai aumentando, maior se torna a dificuldade deste gerenciamento [14].

3.5.3 Hierárquica

Esta arquitetura é a mais utilizada atualmente, principalmente quando se trata de grandes organizações. Diferentemente dos dois modelos apresentados anteriormente, no modelo de ICP Hierárquica existem mais ACs pertencentes a mesma ICP para prover serviços. Desta forma, as ACs nesta arquitetura são organizadas na forma de árvore com um ponto comum de confiança chamado AC Raiz.

Nesta arquitetura, a AC Raiz, além de ser responsável pela emissão de seu próprio certificado, emite também certificados de outras ACs, chamadas ACs subordinadas, que por sua vez podem emitir certificados para usuários ou outras ACs e assim por diante. A AC Raiz normalmente não emite certificados para usuários finais, emitindo

apenas certificados para outras ACs. A criação da estrutura apresentada na Figura 3.3, foi feita a partir da realização dos seguintes passos:

a) A AC_{raiz} emite, além de seu próprio certificado, os certificados das ACs AC_2 e AC_3;

b) A AC_3 emite vários certificados de entidades finais. A AC_2 emite os certificados das ACs AC_4 e AC_5;

c) As ACs AC_4 e AC_5 emitem vários certificados de entidades finais;

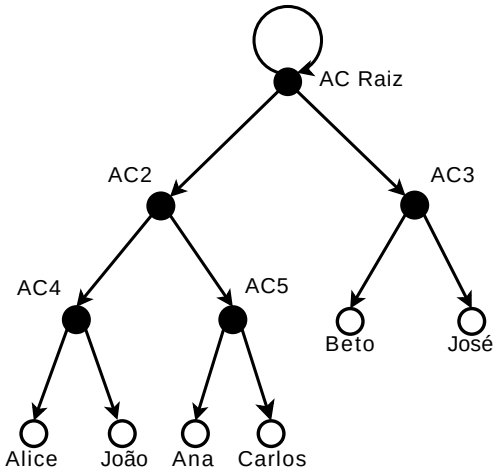

Figura 3.3: Exemplo de uma arquitetura de ICP baseada em Estrutura Hierárquica.

Nesta arquitetura o usuário confia em um único ponto, que é o certificado auto-assinado da AC raiz. Ao confiar na AC raiz, ele passa a confiar em todos os certificados emitidos por ela. A montagem do caminho de certificação é simples, pelo fato de que o certificado de cada AC possui informações referentes à AC que a emitiu, e consequentemente pode-se estabelecer todo o caminho através da hierarquia até que se chegue ao ponto de confiança.

No exemplo da Figura 3.3, se Alice, que confia na AC_{raiz}, deseja verificar o certificado de Beto, ela pode seguir os seguintes passos:

a) A partir do certificado de Beto, Alice obtém informações sobre seu emissor e obtém AC_3;

b) A partir de AC_3, Alice chega ao ponto de confiança, que é a AC_{raiz} e consequentemente verifica que o certificado de Beto é confiável;

Embora seja simples, a verificação do caminho de certificação neste modelo apresenta um considerável aumento no número de certificados e informações a serem verificadas se comparado ao modelo de AC Única. A quantidade de certificados, LCRs e restrições a serem verificadas aumenta de acordo com o número de ACs encontradas no caminho de certificação.

Além de ser mais escalável em relação aos modelos apresentados anteriormente, a arquitetura hierárquica permite também uma melhor distribuição de funções e delegação de tarefas entre as entidades envolvidas na hierarquia. Por exemplo, em uma mesma hierarquia, pode existir um AC que emite apenas certificados digitais para uso de email, outra que emita apenas certificados para uso em servidores, etc. Desta forma, as tarefas de gerência e manutenção de toda a ICP se tornam mais simples e mais organizadas.

Outra vantagem deste modelo pode ser verificada nos casos de comprometimento de alguma AC. No modelo de AC Única, caso a AC seja comprometida, todos os certificados emitidos por ela, inclusive o próprio certificado da AC, terão obrigatoriamente que ser reemitidos. Já no caso da arquitetura hierárquica, caso o comprometimento ocorra em alguma AC subordinada, o impacto sobre a ICP como um todo torna-se muito menor, já que apenas os certificados emitidos por esta AC estão sujeitos a reemissão. No caso de comprometimento da AC Raiz, a única solução encontrada até o presente momento é reemitir todos os certificados da ICP, gerando um impacto semelhante ao comprometimento de uma AC Única. No decorrer deste trabalho serão apresentados novos métodos que tratam este problema de maneira mais adequada, reduzindo significativamente este impacto.

3.5.4 Malha

A arquitetura em Malha trata-se de uma alternativa ao uso da arquitetura hierárquica. A principal diferença entre as duas alternativas está na forma em que as ACs se relacionam. Enquanto no modelo hierárquico todos os usuários possuem o mesmo ponto de confiança e as ACs se estruturam em uma hierarquia, no modelo em Teia, os usuários, embora tenham apenas um ponto de confiança, não necessariamente confiam em uma mesma AC. Neste modelo as relações de confiança não se estabelecem através das relações entre as ACs, que se dão através da emissão de certificados de umas

para as outras, criando uma relação bidirecional. A Figura 3.4 apresenta um exemplo de arquitetura em malha.

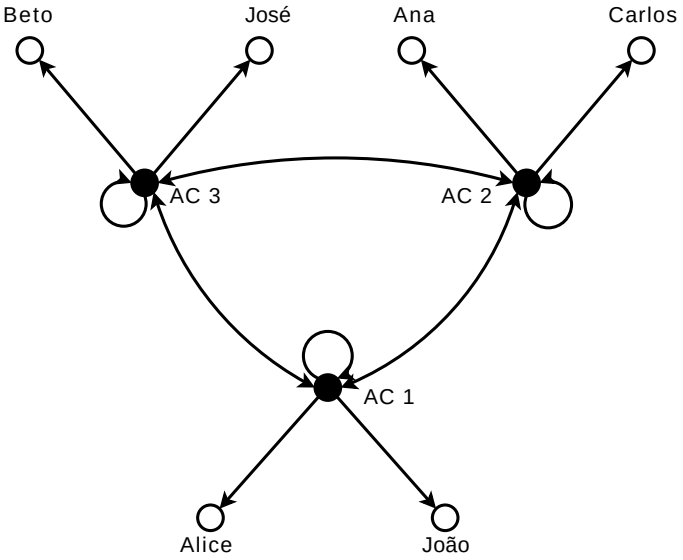

Figura 3.4: Arquitetura de ICP baseada em Estrutura em Malha.

Para se criar uma arquitetura em malha é bastante simples, basta que duas ou mais ACs emitam certificados umas para as outras a fim de que se obtenha um par de certificados que indiquem a relação. Para adicionar uma nova AC no exemplo apresentado na Figura 3.4, basta seguir os seguintes passos:

a) a nova AC (AC_{nova}) inicia o estabelecimento de relação com no mínimo um das ACs já pertencentes à malha, por exemplo a AC_1;

b) a AC_{nova} e AC_1 emitem certificados cruzados entre as duas entidades;

Uma desvantagem que pode ser encontrada neste modelo ocorre quando é realizada a verificação do caminho de certificação, pois trata-se de um processo não determinístico. Este não determinismo dificulta a montagem do caminho pelo fato de existirem múltiplas opções, que podem levar tanto a caminhos corretos quanto a caminhos inválidos, fazendo com que seja necessário reiniciar o processo de montagem [14]. Outra desvantagem ocorre quando o número de ACs envolvidas no processo se torna elevado, pois o número de relações de confiança se torna muito grande e dificulta a sua gerência.

A forma como é estruturada a arquitetura em malha traz uma grande vantagem em relação ao comprometimento de ACs. Quando uma AC é comprometida,

apenas os usuários desta AC são afetados, o restante da ICP permanece inalterado. O relacionamento da AC comprometida com as outras ACs pode ser facilmente removido através da revogação dos certificados emitidos para esta AC sem gerar nenhum outro impacto sobre a ICP além da remoção desta AC.

3.5.5 Lista Estendida de Confiança

A arquitetura de Lista Estendida de Confiança vem para suprir as necessidades encontradas com o uso das Listas de Confiança. Semelhantemente as listas de confiança, o usuário possui uma lista de ACs nas quais confia, e conseqüentemente confia no caminho de certificação destas ACs. Porém no caso da lista estendida de confiança, a ICP em que se confia pode ser de diferentes arquiteturas, como AC Única, Hierárquica ou qualquer outra, fazendo com que esta seja uma arquitetura híbrida como se pode observar na Figura 3.5.

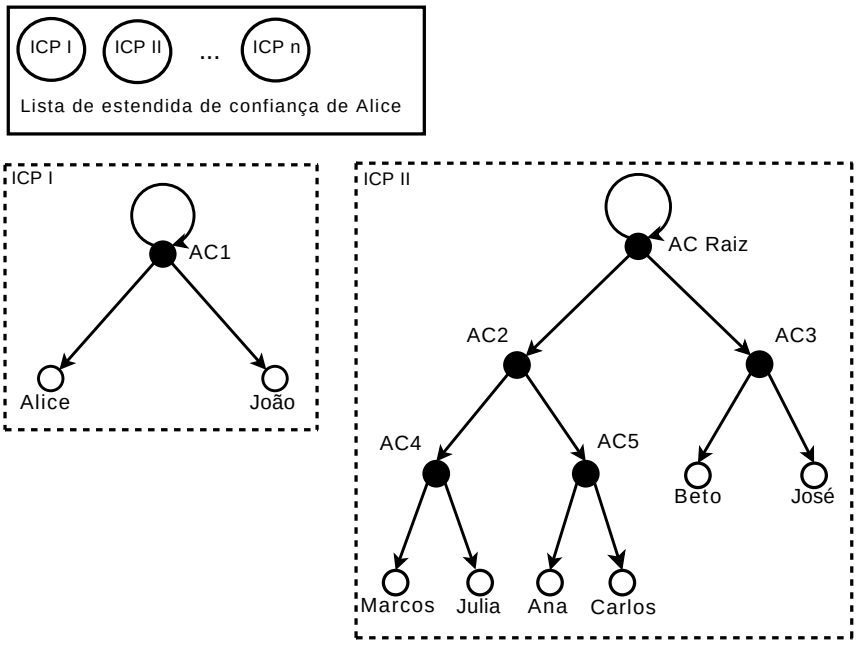

Figura 3.5: Exemplo de arquitetura de ICP baseada em Lista Estendida de Confiança.

Devido ao fato do usuário escolher e gerenciar seus pontos de confiança, este passa a estar sujeito às mesmas desvantagens apresentadas nas listas de confiança. As ICPs presentes na lista do usuário não possuem nenhum controle sobre quem confia nela, e conseqüentemente o usuário pode não ser notificado corretamente sobre comprometimento, revogação ou qualquer outra informação relevante sobre a ICP. Além disso, a

dificuldade na construção do caminho de certificação é maior pelo fato de existirem diferentes arquiteturas, prováveis não determinismos dependendo dos tipos de arquiteturas encontradas na lista e vários possíveis pontos de partida.

3.5.6 Certificação Cruzada

A arquitetura de Certificação Cruzada é uma forma bastante comum de estabelecer relações de confiança entre duas ICPs. Este estabelecimento de confiança se dá através da emissão de certificados cruzados entre ICPs. Para estabelecer certificação cruzada entre n ICPs, é necessário o estabelecimento de $\frac{(n^2-n)}{2}$ relações e a assinatura de $(n^2 - n)$ certificados. A Figura 3.6 representa uma arquitetura utilizando certificação cruzada.

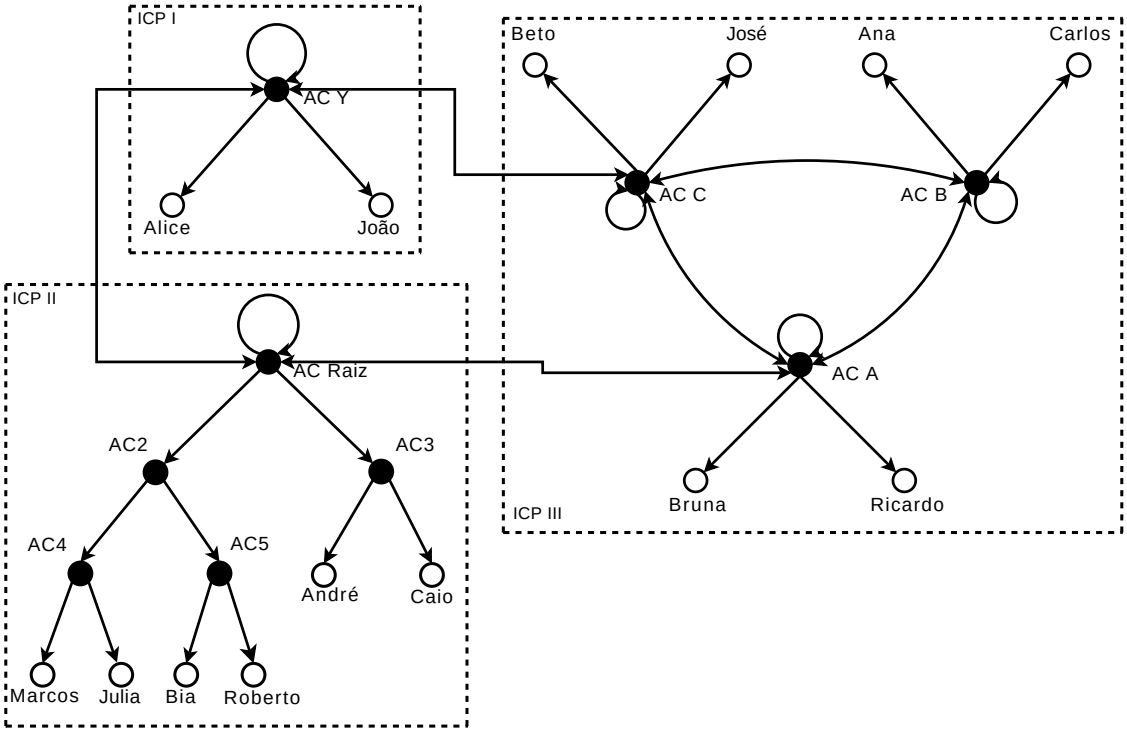

Figura 3.6: Exemplo de arquitetura de ICPs baseada em Certificação Cruzada.

O formato apresentado pela arquitetura de Certificação cruzada mantém do ponto de vista do usuário, um único ponto de confiança. Além disso, retira a responsabilidade de decisão sobre os relacionamentos de confiança por parte do usuários. Cabe aos responsáveis pelas entidades a decisão sobre o estabelecimento de confiança ou não sobre outras ACs, e consequentemente, esta decisão deixa de atingir somente um usuário

e passa a ser válida para todos os usuários de uma ICP.

Por se tratar de uma arquitetura híbrida, esta arquitetura está sujeita as mesmas dificuldades de ICPs com arquiteturas semelhantes. Uma delas trata-se da construção do caminho de certificação que, apesar de solucionar o problema encontrado nas listas de confiança estendida, sendo possível encontrar o caminho de certificação a partir de um único ponto de confiança, deve-se considerar que podem existir diferentes arquiteturas dentro desta ICP, gerando assim possíveis não determinismos.

O comprometimento das chaves de uma AC é tratado de maneira mais eficiente nesta arquitetura. Isto se deve principalmente ao fato de cada usuário possuir apenas um ponto de confiança, deixando a tarefa de gerenciar os problemas referentes às ACs para os administradores. Por sua vez, existe uma relação direta entre as ACs com certificação cruzada, desta forma, se uma AC é comprometida as outras serão notificadas e cada uma delas fica responsável por notificar o comprometimento a seus usuários e tomar quaisquer outras ações relativas à remoção da relação.

3.5.7 Certificação em Ponte

A arquitetura de Certificação em Ponte surgiu com objetivo resolver os problemas que as arquiteturas de Lista Estendida de Confiança e de Certificação Cruzada possuem quando se trata da manipulação de um grande número de pontos de confiança tanto por usuários quanto por administradores de ACs.

A partir desta necessidade, foi criado o conceito de AC Ponte que atua com a função de facilitar o estabelecimento de confiança entre ACs e principalmente diminuir o número de relações necessárias entre ACs apresentadas nas arquiteturas anteriores. A AC Ponte não representa nenhuma relação hierárquica com as ACs com que possui relação e não emite nenhum outro tipo de certificado além dos necessários para a certificação cruzada. A Figura 3.7 apresenta um exemplo de certificação em ponte.

Como resultado da criação desta AC para intermediar as relações de confiança, o número de certificações cruzadas cai de $\frac{(n^2-n)}{2}$ no caso de certificação cruzada, para apenas n, reduzindo significativamente o número de pontos de confiança a serem gerenciados.

Nesta arquitetura, novamente o usuário possui apenas um ponto de confiança, agregando todas as vantagens já citadas anteriormente sobre esta condição.

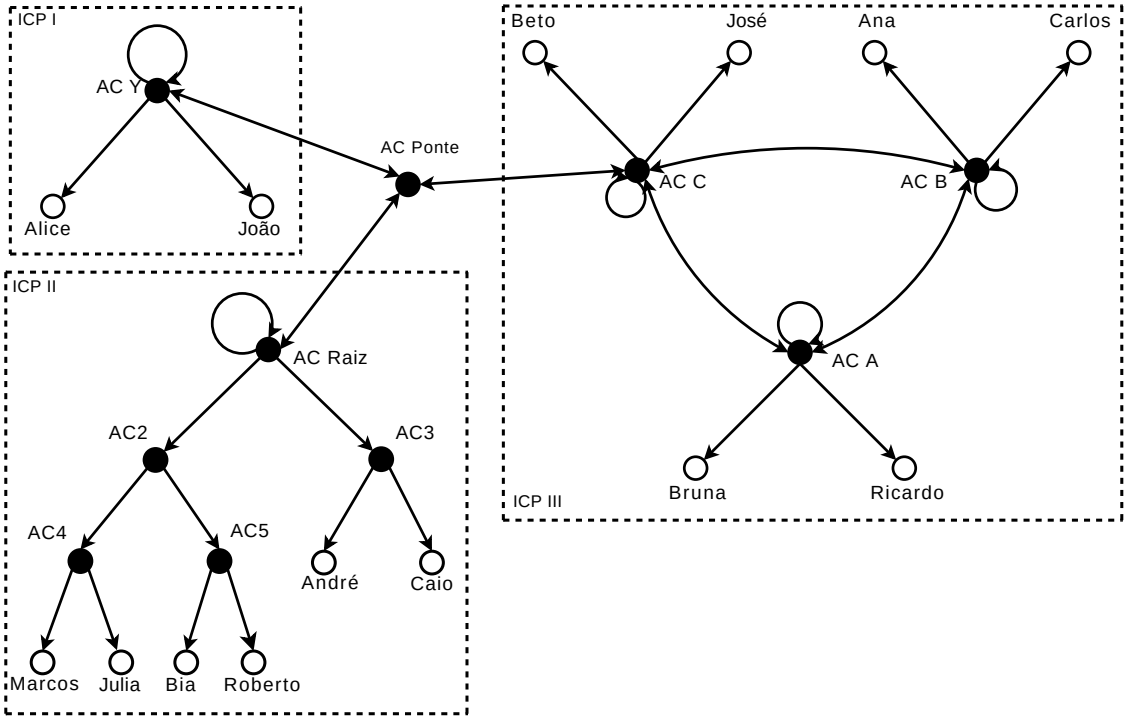

Figura 3.7: Exemplo de arquitetura de ICPs baseada em Certificação em Ponte.

Quando se trata da construção do caminho de certificação, as condições apresentadas são as mesmas referentes à arquitetura em malha.

No caso do comprometimento de ACs, se a AC comprometida não for a AC Ponte, basta a revogação desta entidade por parte da AC Ponte, fazendo com que a ICP a qual pertence a AC comprometida seja removida da relação de confiança com todas as outras ICPs. Já no caso da AC Ponte ser comprometida, cabe a ela a notificação do comprometimento a todas as ACs relacionadas, sendo que ao serem notificadas, estas ACs devem revogar os certificados referentes a esta certificação cruzada. Como resultado desta operação, haverão várias ICPs desconectadas, porém totalmente funcionais dentro de seu escopo. Para o restabelecimento das relações de confiança, basta que se crie uma nova AC Ponte e que se recriem todas as relações.

3.6 Caminho de Certificação

Para que um certificado digital seja considerado válido e consequentemente seja aceito por um usuário, deve haver uma verificação de seus dados a fim de que se possa ter a clara definição que esta entidade representada pelo certificado é realmente

quem ela clama ser.

Esta verificação baseia-se na tentativa de estabelecimento de um caminho de certificação entre o certificado a ser verificado e uma entidade na qual o usuário que está realizando a verificação confie previamente. Além disso, cada certificado pertencente a este caminho de certificação deve ser verificado.

Apesar de não ser um processo padronizado e com poucas referências na literatura, de um modo geral o processamento do caminho de certificação consiste em duas etapas: [27]

Construção – onde um ou mais possíveis caminhos são construídos;

Validação – onde são verificados em cada certificado do caminho de certificação itens como: validade, situação de revogação, integridade e quaisquer outras restrições definidas.

3.6.1 Construção do Caminho de Certificação

A construção do caminho de certificação compreende a busca pela cadeia de certificados entre o certificado a ser verificado e um ponto de confiança reconhecido. Esta ação pode ser realizada de duas formas: uma direta, partindo da entidade final para o ponto de confiança; e inversa, partindo do ponto de confiança para a entidade final.

Pode-se dividir os critérios de montagem do caminho de certificação de acordo com os parâmetros utilizados para a realização do encadeamento. Com isso, surgem dois principais tipo de encadeamento: o encadeamento por nome e o encadeamento por identificador de chave [27].

3.6.1.1 Encadeamento por nome

Neste tipo de encadeamento, monta-se o caminho de certificação entre o ponto de confiança e o certificado. Partindo do ponto de confiança para o certificado a ser validado, a cadeia é montada verificando se o campo “sujeito” do certificado atual é igual ao campo emissor do próximo certificado da cadeia, e assim sucessivamente. Do mesmo modo, partindo do certificado a ser validado para o ponto de confiança, a validação se faz através da comparação do campo emissor do certificado atual com o campo sujeito

do próximo certificado da cadeia e assim por diante. A figura 3.8 apresenta este tipo de validação.

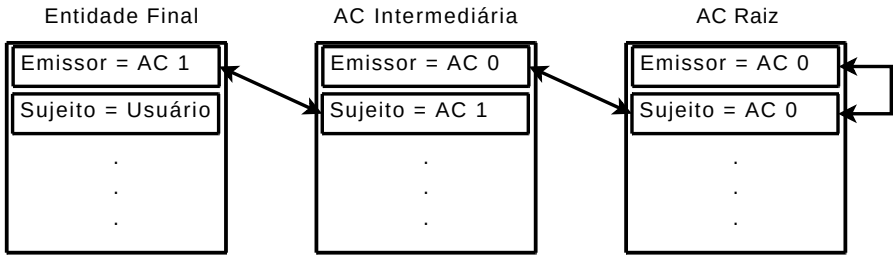

Figura 3.8: Construção do caminho de certificação através de encadeamento por nome

Este método mostra-se bastante satisfatório quando se há garantia de que todas as ACs envolvidas na construção do caminho de certificação possuam apenas um par de chaves. Porém existem várias situações onde em um determinado momento uma AC pode possuir mais de um par de chaves.

Quando uma AC emite certificados de transição de chaves [2] (mais detalhes sobre certificados de transição de chaves serão vistos na seção 4.1), o encadeamento por nome pode não ser suficiente, pois por um determinado período de tempo passa a ter simultaneamente certificados digitais com o mesmo nome, e com diferentes pares de chaves.

A partir desta situação, o encadeamento apenas por nome pode não ser suficiente para a montagem de um caminho de certificação válido, fazendo com que seja necessária uma nova forma de se construir este caminho baseada na identificação da chave do certificado, e não no nome. Com a terceira versão de certificados X.509, tornou-se possível a adição de extensões aos certificados digitais, e para facilitar a montagem do caminho de certificação foram criadas duas novas extensões, o “Subject Key Identifier” (SKID) e “Authority Key Identifier” (AKID).

3.6.1.2 Encadeamento por Identificador de Chave

A montagem do caminho de certificação a partir da utilização do encadeamento por identificador de chave é realizada de maneira semelhante a do encadeamento por nome, diferindo pelo fato que a verificação se dá pelo valor do *Subject Key Identifier* (SKID) e do *Authority Key Identifier* (AKID) que são extensões de certificados utilizadas com a finalidade de facilitar o processo de construção do caminho de certifica-

ção [28]. Portanto, utilizando a construção na forma direta, AKID do primeiro certificado deve ser igual ao SKID do próximo e assim por diante; já na forma inversa, o SKID do primeiro certificado deve ser igual ao AKID do próximo certificado. A figura 3.9 apresenta um exemplo de como realizar a construção do caminho de certificação a partir do identificador de chave. As linhas tracejadas indicam que o campo AKID na AC Raiz pode existir em alguns casos e em outros não.

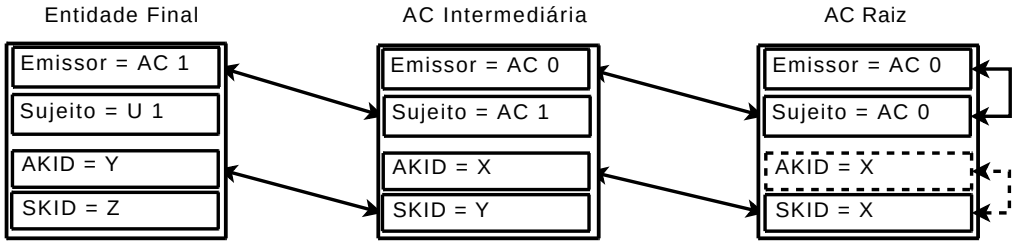

Figura 3.9: Construção do caminho de certificação através de encadeamento por AKID

O *Authority Key Identifier* é um extensão não-crítica que provê meios de identificar a chave pública correspondente à chave privada utilizada para assinar um certificado quando uma AC possui múltiplas chaves de assinatura. Esta identificação pode ser baseada no identificador da chave, ou no nome do emissor juntamente ao seu número serial.

A estrutura ASN.1 [29] da extensão AKID é definida da seguinte forma:

```
AuthorityKeyIdentifier ::= SEQUENCE {
   keyIdentifier             [0] KeyIdentifier           OPTIONAL,
   authorityCertIssuer       [1] GeneralNames            OPTIONAL,
   authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL  }

KeyIdentifier ::= OCTET STRING
```

Embora os campos *keyIdentifier*, *authorityCertIssuer* e *authorityCertSerialNumber* de acordo com a estrutura apresentada acima sejam opcionais, a RFC 3280 determina que o campo *keyIdentifier* deve ser incluído em todos os certificados emitidos por ACs conformes, para facilitar a construção do caminho de certificação. A única exceção ocorre no caso de certificados auto-assinados, onde a extensão *Authority Key Identifier* pode ser omitida [1].

Além disso, uma definição contida no padrão X.509 merece destaque neste contexto:

> "O *keyIdentifier* pode ser utilizado para selecionar certificados durante a construção do caminho. O par *authorityCertIssuer, authoritySerialNumber* podem ser utilizados apenas para prover preferência para um certificado sobre outros durante a construção do caminho de certificação."

O valor do campo *keyIdentifier* pode ser calculado de várias formas, sem que nenhum método seja considerado obrigatório. O valor mais comum atribuído a este campo é a seqüência de 20 bytes resultantes da aplicação da função de resumo criptográfico SHA-1 sobre o valor da chave pública do sujeito. Já o valor do campo *authorityCertIssuer* deve ser igual ao valor do campo *Issuer* do certificado do emissor. O valor do campo authorityCertSerialNumber deve ser igual ao valor do campo *serialNumber* do certificado do emissor.

O *Subject Key Identifier* é uma extensão não crítica que provê meios de identificar certificados que contém uma determinada chave pública. A estrutura ASN.1 [29] da extensão SKID é definida da seguinte forma:

```
SubjectKeyIdentifier ::= KeyIdentifier
```

De acordo com a RFC 3280, a extensão *SubjectKeyIdentifier* deve estar presente em todos os certificados de autoridades certificadoras.

Após a apresentação dos conceitos e das definições aplicadas às extensões SKID e AKID, podemos concluir que a montagem do caminho de certificação por encadeamento por identificador de chave é realizada da seguinte forma quando se utiliza a forma direta:

- compara-se o valor do campo *keyIdentifier* contido na extensão AKID do primeiro certificado com o valor do campo *keyIdentifier* da extensão SKID do próximo certificado, e assim sucessivamente;

- caso sejam encontrados mais de um certificado com o mesmo valor do campo *keyIdentifier* como provável integrante do caminho de certificação, pode-se considerar o valor dos campos *authorityCertIssuer* e *authoritySerialNumber* para definição da escolha do certificado e consequentemente dar continuidade ao processo de montagem. De qualquer forma, esta escolha não deve excluir o(s) certificado(s) não selecionados através deste critério como candidatos a montagem do caminho de

certificação, e caso o certificado escolhido não leve ao ponto de confiança, estes certificados podem ser escolhidos para novas tentativas de montagem.

A figura 3.10 representa o que foi descrito acima. As setas representam comparações entre campos que devem obrigatoriamente ser iguais. As linhas tracejadas representam comparações entre campos que podem apenas definir preferência entre um certificado ou outro.

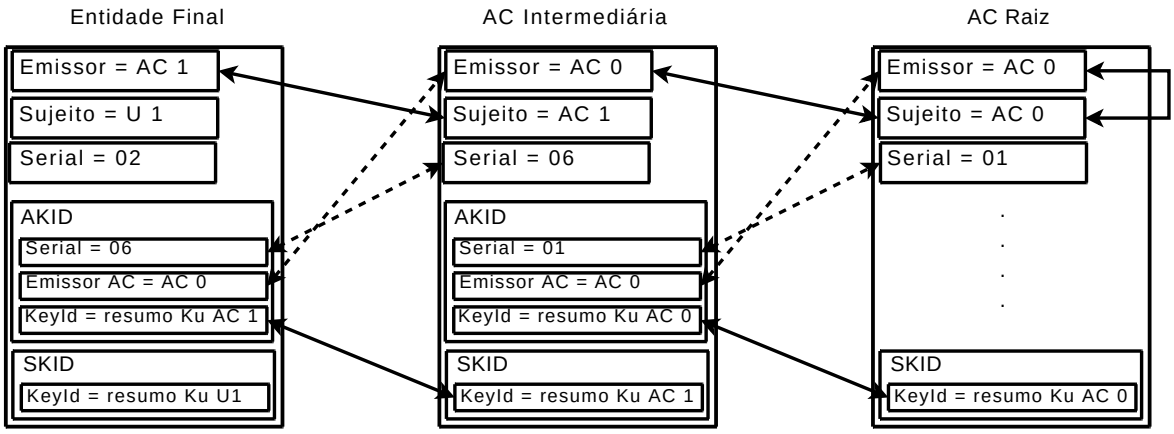

Figura 3.10: Construção do caminho de certificação através de encadeamento por AKID completo

3.6.2 Validação do Caminho de Certificação

Após a determinação dos possíveis caminhos de certificação entre o certificado e o ponto de confiança, é necessário realizar a validação deste caminho, ou seja, verificar se todos os certificados estão válidos, não foram revogados, etc.

Para que a validação seja realizada, cada certificado do caminho de certificação deve passar pelas seguintes verificações:

Assinatura digital – verificar se a assinatura digital do certificado está correta e se este foi realmente assinado pela AC de nível imediatamente superior no caminho de certificação. No caso do certificado auto assinado, a verificação é realizada com a chave pública do próprio certificado.

Data de validade – se o certificado se encontra dentro de seu período de validade.

Nomes – se o nome presente no campo emissor do certificado é igual ao campo sujeito do certificado de nível imediatamente superior no caminho de certificação.

Situação de revogação – Se o certificado não está revogado.

Restrições básicas – Todos os certificados intermediários devem ter o campo *CA* da extensão *basic constraints* marcado como *true*. Se a o campo *pathLenConstraint* existir, verificar se seu valor está sendo respeitado.

Restrições de políticas – verificar todas as restrições políticas aplicáveis ao certificado.

Restrições de nomes – verificar todas as restrições de nomes aplicáveis ao certificado.

Extensões Críticas – reconhecer e processar todas as extensões críticas presentes no certificado;

Caso alguma das validações acima falhar, o caminho de certificação é considerado inválido. Se todos os certificados forem aprovados em todas as validações, o caminho de certificação é considerado válido.

3.7 Conclusão

Conforme o que foi apresentado no decorrer do capítulo, a criptografia, embora possa individualmente atender os requisitos de segurança de seus usuários, ao ser aplicada em grande escala e em ambientes distribuídos, necessita de mecanismos para ser gerenciada de maneira mais eficiente. A infra-estrutura de chaves públicas tem a capacidade de suprir esta necessidade, e também de relacionar entidades às suas respectivas chaves.

Quem desempenha a função de relacionar uma chave a uma entidade são as Autoridades Certificadoras, as quais atestam que um determinado de conjunto de informações relacionadas a uma chave pública pertecem a uma entidade. Com isso, a necessidade de que uma AC e seu par de chaves estejam sempre disponíveis é de vital importância para o bom funcionamento de toda a infra-estrutura. Para que eventuais situações que tornem tanto os certificados de uma AC quanto suas chaves indisponíveis, deve-se possuir mecanismos de reestabelecimento de sua disponibilidade de maneira rápida, eficiente e que afete o menor número de entidades vinculadas a ela.

Este capítulo serve como base para todo o conteúdo discutido no decorrer desta dissertação.

Capítulo 4

Substituição de Chaves e Certificados de uma AC

Atualmente existem alguns métodos que indicam como tratar a necessidade da troca do par de chaves de uma Autoridade Certificadora. Este capítulo descreve detalhadamente cada um desses métodos.

4.1 Protocolo de Gerenciamento de Certificados

O Protocolo de Gerenciamento de Certificados (*Certificate Management Protocol* – CMP) compreende uma série de procedimentos e estruturas de dados que envolvem emissão, revogação, renovação e atualização de certificados digitais. Um de seus procedimentos, define o mecanismo de troca do par de chaves de uma Autoridade Certificadora Raiz.

Para apresentar um novo certificado digital ou uma nova chave de assinatura de listas de certificados revogados (LCR), uma AC deve emitir certificados de transição [2, 14] para o antigo e novo par de chaves. Os certificados de transição são necessários para que os subscritores de certificados pertencentes a uma ICP possam construir um caminho de certificação válido para certificados pertencentes à mesma ICP, mas assinados com uma nova chave privada (KR_{nova}).

O procedimento básico consiste em guarnecer a nova chave pública (KU_{nova}) utilizando a antiga chave privada (KR_{velha}) e vice-versa, conforme ilustra a Figura 4.1. As setas representam certificados, os círculos preenchidos representam Auto-

ridades Certificadoras e os círculos sem preenchimento representam entidades finais.

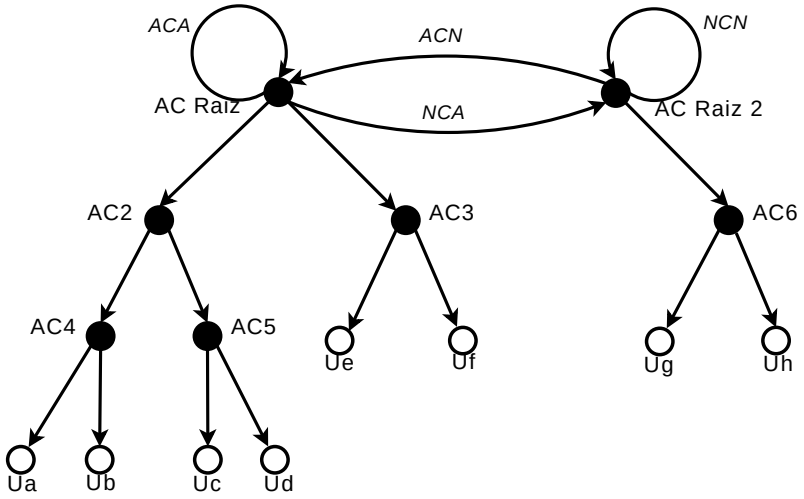

Figura 4.1: Estrutura hierárquica após troca do par de chaves da AC Raiz. As linhas tracejadas indicam que os certificados são semelhantes ao da origem e não uma hierarquia. ACN é a AC *Antiga-com-Nova*, NCA é a AC *Nova-com-Antiga*, ACA é a AC *Antiga-com-Antiga*, NCN é a AC *Nova-com-Nova*.

Para a realização deste processo, são gerados 3 novos certificados: o certificado da nova AC Raiz e dois certificados de transição: o certificado NCN (Novo com Novo) para a nova AC Raiz (RCA_2), os certificados de transição ACN (Antigo com Novo) e NCA (Novo com Antigo). Ao final do processo, existirão 4 certificados da mesma AC: o antigo (*Antigo-com-Antigo*); o novo (*Novo-com-Novo*); o antigo assinado com a nova chave privada (*Antigo-com-Novo*); e o novo assinado com a antiga chave privada (*Novo-com-Antigo*) [2].

Os passos para a realização da substituição da chave de uma AC utilizando este protocolo são:

a) criar um novo par de chaves;

b) emitir o certificado Antigo-com-Novo – certificado assinado pela nova chave privada contendo a antiga chave pública;

c) emitir o certificado Novo-com-Antigo – certificado assinado pela antiga chave privada contendo a nova chave pública;

d) emitir o certificado Novo-com-Novo – certificado assinado pela nova chave privada contendo a nova chave pública;

e) publicar os novos certificados nos repositórios e de outras possíveis maneiras.

Ao final do processo, a chave privada antiga não é mais necessária, já a chave pública permanecerá em uso (para uso além de verificações de não repúdio e caminho de certificação) até que todas as entidades finais tenham recebido de forma segura a nova chave pública [2].

O certificado *Antigo-com-Antigo* é o certificado original. O certificado *Novo-com-Novo* deve ter validade iniciando no momento de criação do novo par de chaves e se encerrando no momento em que a AC atualizará novamente seu par de chaves.

O certificado *Antigo-com-Novo* (ACN) contém a chave pública do certificado antigo, e é assinado pela nova chave privada. Desta forma, é possível aos detentores de certificados assinados pela nova chave privada, a construção de um caminho de certificação válido para os certificados assinados com a chave privada antiga [14]. O período de validade deste certificado se inicia no momento em que o certificado é emitido e se encerra na mesma data em que vence o certificado que contém a chave pública antiga.

O certificado *Novo-com-Antigo* (NCA) contém a chave pública do certificado novo, e é assinado pela chave privada antiga. Assim, os detentores de certificados assinados pela chave privada antiga podem construir um caminho de certificação válido para os certificados assinados com a nova chave privada [14]. O período de validade se inicia no momento em que o certificado é emitido e tem como data de validade o tempo necessário para que todas as entidades desta AC possuam a nova chave pública, que no pior caso, será a data de validade da chave pública antiga [2].

Como se pode notar, o modelo apresentado é bastante semelhante a arquitetura de certificação cruzada discutida na seção 3.5.6, e consequentemente possui vantagens e desvantagens semelhantes. A implicação mais clara neste caso é a geração de não determinismos na construção do caminho de certificação, o que implica em um aumento no custo da montagem do caminho de certificação entre usuários pertencentes a mesma ICP, porém com pontos de confiança distintos (ACA e NCN).

No caso de comprometimento da chave do certificado ACA, este modelo não se mostra aplicável, uma vez que a confiança na chave privada antiga deixa de existir. A RFC 4210 não indica nenhuma forma de proceder caso esta situação ocorra, porém como se trata de um caso onde a disponibilidade e confiança na chave antiga são de fundamental importância, pode-se concluir que não há maneiras de tratar esta situação

para que seja possível aplicar este método.

4.2 Lista de Certificados Confiáveis

As Listas de Certificados Confiáveis (*Certificate Trust List* – CTL) foram inicialmente criadas como um mecanismo de estabelecimento de confiança em certificação cruzada a fim de evitar a necessidade do uso de diretório [30]. Além desta aplicação, as CTL podem ser também utilizadas como parte integrante de um mecanismo de transição do ponto de confiança de uma ICP.

Trata-se de um conteúdo assinado utilizando o formato PKCS#7 [31] que contém informações sobre políticas, período de validade, extensões e uma lista dos resumos criptográficos dos certificados confiáveis. A estrutura ASN.1 de uma CTL é apresentada abaixo:

```
CertificateTrustList ::= SEQUENCE {
     version               Version DEFAULT v1,
     subjectUsage          Subject Usage,
     listIdentifier        ListIdentifier     OPTIONAL,
     sequenceNumber        INTEGER            OPTIONAL,
     thisUpdate            ChoiceOfTime,
     nextUpdate            ChoiceOfTime
     subjectAlgorithm      AlgorithmIdentifier,
     trustedSubjects       TrustedSubjects,
     extensions            Extensions         OPTIONAL }
```

Para suprir a necessidade de apresentação de um novo certificado ou de novas chaves de AC, basta adicionar o hash do novo certificado na CTL da AC antiga. Desta forma, as entidades que confiam na chave desta AC, passam a confiar na chave da nova AC no momento em que adquirem a CTL assinada pela AC antiga. O processo de apresentação do novo certificado e chave pode ser visualizado na figura 4.2 e segue os seguintes passos: [32]

a) Cria-se o certificado atualizado da AC (AC_{nova});

b) A AC_{antiga} obtém o certificado da AC_{nova};

c) A AC_{antiga} cria uma CTL assinando-a com sua chave privada, incluindo o hash do certificado da AC_{nova};

d) A AC_{antiga} pública a CTL em um repositório (LDAP, HTTP, etc);

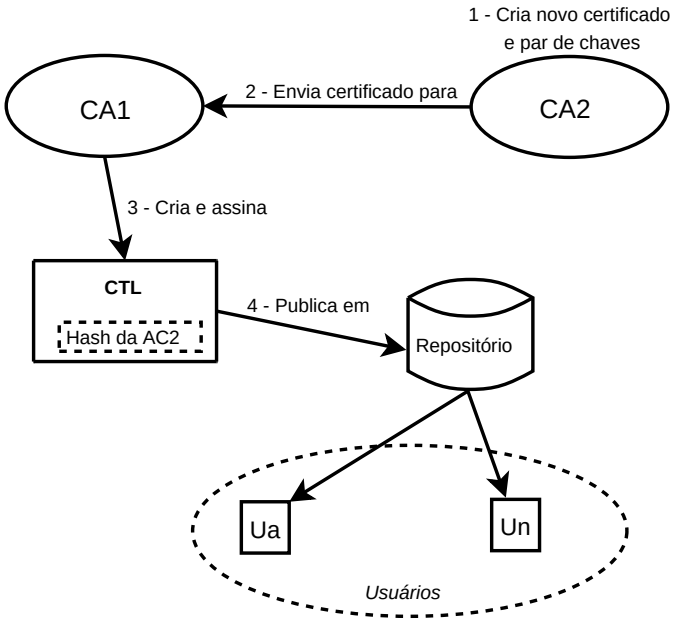

Figura 4.2: Processo de apresentação de um novo certificado e nova chave utilizando CTL

Desta forma, os subscritores da AC_{antiga} passam a confiar nos certificados emitidos pela AC_{nova}, pois a CTL emitida estabelece a confiança entre as ACs. De qualquer maneira, diferentemente do CMP, as ACs nova e antiga não tem relação direta em sua topologia, o que implica na existência da necessidade de sempre ter disponível a CTL no momento de verificação de estabelecimento de confiança entra duas ACs.

Este modelo mostra-se bastante semelhante às Listas estendidas de confiança apresentadas na seção 3.5.5, porém quem é o responsável pela lista de confiança não é o usuário e sim a Autoridade Certificadora. Com esta diferença, os problemas relativos a gerência de informação por parte do usuário deixam de existir, e a notificação de comprometimento da entidade ou qualquer outra informação crítica se torna mais fácil de ser notificada. Como desvantagem, pode-se dizer que este mecanismo padece de dificuldades semelhantes às das LCRs, uma vez que ambas são listas publicadas pela autoridade certificadora a fim de fornecer informações sobre certificados aos usuários.

No caso de comprometimento da chave do certificado AC_{antiga}, semelhantemente ao CMP, este modelo não se mostra aplicável, uma vez que a confiança na

chave privada antiga deixa de existir. Diferentemente do CMP, este método pode também ser aplicado na atualização do certificado digital da uma AC sem que a chave seja atualizada. O processo para a realização desta atualização é igual ao descrito acima para a substituição de chaves criptográficas.

4.3 Conclusão

No decorrer deste capítulo foram apresentados os métodos atualmente disponíveis na literatura para substituição de Chaves e Certificados de uma Autoridade Certificadora. De maneira geral, os métodos apresentados mostram-se eficientes para a atualização do certificado e do par de chaves de uma ICP, porém ambos os métodos utilizam obrigatoriamente a chave privada da AC antiga. Com isso, pode-se notar que existe uma situação de grande relevância para uma ICP que não é tratada corretamente nestes métodos, a qual ocorre quando a antiga chave privada não está mais disponível. Esta e outras situações serão tratadas no próximo capítulo.

Capítulo 5

Substituição Dinâmica de Chaves e Certificados

Os métodos descritos no capítulo 4 descrevem os procedimentos a serem realizados quando há a necessidade de troca do par de chaves da AC Raiz. Estes métodos, embora bastante funcionais, não possuem toda a abrangência necessária para cumprir todos os requisitos de uma ICP durante seu ciclo de vida. Seu objetivo é a simples substituição da chave privada da AC raiz.

Nenhum dos métodos apresentados aborda a simples atualização do certificado, sem a necessidade da troca do par de chaves. Outra questão que se mostra relevante é quando se trata de atualização de certificados ou de substituição do par de chaves. A prática mostra que existem diferentes necessidades para diferentes ICPs, dificultando assim a utilização de um único método.

Nesta seção serão apresentados, em detalhes, novos modelos que atendem diversas situações de substituição de AC. Como já discutido, existem dois tipos de operações que, se realizadas em uma AC, podem causar algum impacto em sua topologia, que são a substituição do certificado e a substituição da chave privada. Cada uma dessas alterações possui algumas subdivisões que necessitam ser tratadas de forma diferenciada. No decorrer desta seção, cada uma destas operações será descrita e uma respectiva solução será proposta.

A Figura 5.1 apresenta os tipos de trocas que podem ocorrer com o certificado digital de uma Autoridade Certificadora.

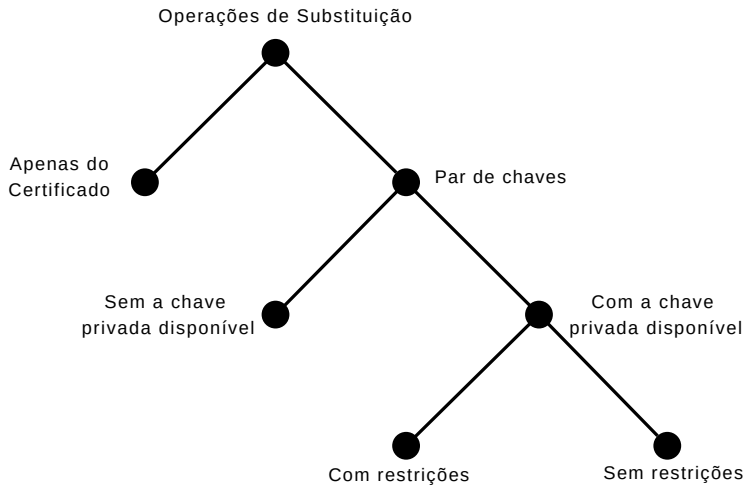

Figura 5.1: Possíveis tipos de trocas de certificados digitais

5.1 Substituição do Certificado

Os certificados possuem um tempo de vida fixo quando são emitidos. Quando se aproxima da data final de validade, é necessária a emissão de um novo certificado [33] e, eventualmente, a geração de um novo par de chaves criptográficas. A substituição de um certificado de AC faz-se necessária por vários motivos. Além da questão do período de validade, pode existir a necessidade de alteração de algum atributo, ou modificação de alguma política. Em todos estes casos, a substituição da chave privada não é necessária caso ela esteja disponível e não exista nenhuma restrição quanto a sua segurança ou política.

Este processo pode ser divido em dois tipos: o de alteração do certificado, que se aplica à necessidade de mudança em algum de seus atributos, e o de renovação, onde embora seja necessária a substituição do certificado, todos os seus atributos são mantidos, com exceção das datas de início e fim de validade.

5.1.1 Alteração do Certificado

A alteração de um certificado digital pode ser necessária por vários motivos, como por exemplo a necessidade de modificação de alguma extensão. Quando uma alteração é realizada em um certificado de entidade final, o processo é bastante simples, bastando a solicitação de um novo certificado e a posterior revogação do certificado antigo. Porém, quando o certificado a ser alterado é de uma Autoridade Certificadora,

a solução não é tão simples, pelo fato de que mais entidades podem ser afetadas se os procedimentos tomados não forem adequados.

Um fator que deve obrigatoriamente ser levado em consideração é a construção do caminho de certificação. Uma alteração em um certificado digital de AC só será bem sucedida se após a realização da alteração, o caminho de certificação para os subscritores desta AC puder ser construído, e apontar para os certificados e entidades corretas. Baseado nesta necessidade, juntamente aos conceitos apresentados na seção 3.6, pode-se chegar a conclusão que é possível alterar um certificado digital de uma Autoridade Certificadora com sucesso, porém existem algumas restrições e alguns campos que não devem ser modificados. São eles:

Sujeito – a construção do caminho de certificação sempre se baseia no valor dos campos Sujeito e Emissor dos certificados, portanto, se este campo for alterado, todos os certificados emitidos por esta AC devem ser reemitidos para que seu campo Emissor seja atualizado, tornando o processo inviável na maioria dos casos. Portanto, o campo sujeito de um certificado de AC só pode ser modificado se a reemissão de todos os certificados emitidos pela AC for viável. Se o campo Sujeito do certificado da AC for modificado e os certificados emitidos por ela não forem reemitidos, o caminho de certificação para todos eles não apontará para o novo certificado;

Extensão *Basic Constraints* – a validação do caminho de certificação invariavelmente inclui a verificação do conteúdo desta extensão caso ela exista. Portanto, toda alteração em seu valor deve ser analisada cuidadosamente a fim de não violar as políticas definidas para a ICP como um todo e também respeitar as definições encontradas no certificado de seu emissor (se houver). Por exemplo: em uma ICP onde partindo-se da AC Raiz até um certificado de entidade final encontramos o caminho $AC_{raiz} \rightarrow AC_A \rightarrow AC_B \rightarrow$ usuário final, onde a AC Raiz possui o valor do atributo *pathLenConstraint* definido como 2, o certificado da AC_A não pode ter o valor de sua extensão *Basic Constraints* alterado, pois obrigatoriamente o valor do atributo *pathLenConstraint* em seu certificado deve ser 1. Se esta restrição não for respeitada, o caminho de certificação pode até ser construído, mas não será aprovado na etapa de validação.

Quaisquer extensões que impliquem em mudanças em restrições de políticas – Da

mesma forma que no item anterior, a validação de um caminho de certificação candidato inclui verificações nas extensões que fazem restrições políticas sobre os certificados. Desta forma, qualquer alteração no valor destas extensões tem chances elevadas de invalidar um caminho de certificação.

Dadas as restrições, o processo de alteração de um certificado digital de uma Autoridade Certificadora é simples. O operador da Autoridade Certificadora deve realizar os seguintes passos:

a) gera-se uma requisição de certificado [34, 35] contendo a chave pública do certificado antigo;

b) se o procedimento for para uma AC Intermediária, submete-se a requisição para a mesma AC que emitiu o certificado antigo e esta emite o certificado, se for para uma AC Raiz, gera-se um certificado auto-assinado;

c) revoga-se o certificado antigo;

d) publica-se os novos certificados nos repositórios e de outras possíveis maneiras.

Após a realização deste procedimento, o certificado antigo deixará de ser válido e apenas o novo certificado será utilizado. Todos os certificados emitidos pela AC passarão a ter seu caminho de certificação construído e validado utilizando o novo certificado.

O maior impacto desta alteração será que os usuários que tinham o certificado antigo como certificado de confiança, deverão obter de alguma forma o novo certificado para que seja possível a construção do caminho de certificação para o novo certificado. Este processo pode ser demorado, dependendo das formas de notificação utilizadas pela AC, e portanto, a alteração de um certificado digital de uma Autoridade Certificadora deve sempre ser analisada com muito cuidado.

5.1.1.1 Construção do caminho de certificação para o novo certificado

A forma como o caminho de certificação para o novo certificado é construído depende das informações contidas nos certificados existentes neste caminho. Se o certificado não possui as extensões *Authority Key Identifier* e *Subject Key Identifier*, a

forma mais utilizada para a construção do caminho é através do encadeamento por nome. Já se o certificado possui tais extensões, a montagem do caminho se dá através do uso conjunto do encadeamento por nome, aliado ao encadeamento por identificador de chave.

Portanto, a construção do caminho de certificação para o certificado alterado pode ser realizada das seguintes formas:

Por nome – como definimos que o nome não será alterado, o encadeamento por nome é realizado diretamente, exatamente como descrito na seção 3.6.1.1.

Por identificador de chave – partindo do certificado de entidade final até o ponto de confiança, a comparação é feita conforme descrito na seção 3.6.1.2. Com isso, serão encontrados dois caminhos candidatos, um deles apontando para o certificado antigo e outro para o novo. Se a extensão AKID do certificado de nível imediatamente inferior ao certificado alterado contiver apenas o campo *keyIdentifier* definido, o caminho de certificação iniciará a fase de validação do caminho a partir do certificado novo, e após a validação, aceitará este caminho como válido. Porém se o AKID contiver os campos *authorityCertIssuer* e *authorityCertSerialNumber* definidos, este valores coincidirão apenas com o certificado antigo, fazendo com que seja dada preferência para este caminho e a etapa de validação seja inicialmente realizada através deste. Após a falha na validação pelo fato do certificado antigo estar revogado, parte-se para a tentativa de validação do caminho utilizando o novo certificado, e este será validado com sucesso.

Os critérios utilizados na escolha entre um caminho de certificação candidato ou outro pode variar. O critério apresentado acima e que será utilizado durante todo restante do trabalho, deriva das definições e normas encontradas na literatura, porém nada impede que para fins de otimização, outros critérios possam ser utilizados para escolher qual o caminho candidato será o primeiro a ser testado na fase de validação, por exemplo, um possível critério a ser selecionado pode ser a opção pelo caminho de certificação mais curto.

5.1.2 Renovação do Certificado

O caso da renovação é mais simples. Diferentemente do caso da alteração do certificado, a renovação não envolve a modificação de nenhum campo do certifi-

cado com exceção de suas datas de validade e número serial. Desta forma, a análise do impacto causado pela modificação dos campos não se faz necessária. Com isso, pode-se observar que a renovação do certificado nada mais é do que um caso particular da alteração apresentada na seção anterior.

Por se tratar de um caso particular da alteração do certificado, os mesmos critérios, definições e procedimentos apresentados no caso de alteração, se aplicam à renovação, com exceção da necessidade de revogação do certificado antigo, sendo este podendo ser mantido válido até que expire.

Por ser mais simples e não precisar de uma análise mais detalhada sobre os impactos das alterações do certificado, este método possibilita que sejam gerados sistemas automatizados para renovação de certificados, reduzindo significativamente a complexidade do processo e consequentemente reduzindo custos, facilitando o processo de emissão e tornando a renovação mais dinâmica.

5.2 Substituição do par de chaves

Quando existe a necessidade de substituição da chave privada de uma AC e a conseqüente troca de seu certificado, podem ocorrer dois casos: um quando a chave privada está disponível; e o outro quando a situação oposta ocorre, ou seja, não se tem acesso à chave. Cada um dos casos requer um tratamento específico e diferenciado com a finalidade de proporcionar o menor impacto possível para a topologia da ICP. A seguir será descrito como proceder na ocorrência de cada um destes casos.

5.2.1 Sem chave privada disponível

A disponibilidade é muito importante quando trata do acesso à chave privada de uma AC. Quando a chave privada não está disponível, seja devido a uma falha no dispositivo que a armazena ou até mesmo por restrições políticas ou físicas sobre seu uso, toda a estrutura é prejudicada. Até o presente momento, a única solução encontrada para este problema é a reemissão de todos os certificados emitidos pela AC e em todos os seus níveis inferiores de sua hierarquia. Tal aplicação pode ser viável e até rotineira em pequenos ambientes, para solucionar problemas como a necessidade de emissão de LCRs [36]. Porém, em ACs onde existe um grande número de certificados emitidos, ou

em ACs que emitem certificados de ACs, este procedimento passa a ser inviável e com custo muito elevado.

Nenhum dos modelos apresentados no capítulo 4 pode ser aplicado neste caso pelo fato da chave privada não estar disponível, e conseqüentemente a AC antiga não poderá assinar os certificados de transição e/ou CTL.

Devido ao fato de não se encontrar na literatura nenhum método eficiente para tratar este problema, surge a necessidade da elaboração de um novo método. Da mesma forma que em todos os procedimentos de substituição de certificados ou chaves de uma AC, este novo método deve necessariamente possuir as seguintes características:

a) deve estabelecer um novo caminho de certificação que seja construído de maneira condizente com as normas atuais;

b) não pode ter como pré-requisito a utilização da chave privada antiga da AC;

c) deve ser possível restabelecer o funcionamento da ICP como um todo de maneira rápida e eficiente;

d) deve ser simples de ser realizado;

e) o impacto sobre a topologia da ICP deve ser mínimo, se restringindo à AC afetada ou no máximo os certificados emitidos por ela;

f) deve utilizar apenas estruturas de dados conhecidas e em uso atualmente, preferencialmente apenas certificados digitais e listas de certificados revogados;

g) a nova AC deve ter condições de realizar as mesmas operações que eram realizadas pela antiga.

A partir dos requisitos apresentados, do estudo detalhado das normas de construção e validação do caminho de certificação e da revisão das soluções existentes, foi elaborada uma nova solução.

No caso de uma ICP já estabelecida, como a apresentada na Figura 5.2, ter a chave privada de sua Autoridade Certificadora Raiz comprometida, deve-se inicialmente criar um novo par de chaves e a partir deste, emitir um novo certificado auto-assinado. Na figura 5.3, esta nova AC é chamada de AC Raiz 2. O novo certificado e o novo par de chaves constituem a nova AC Raiz que será implantada.

Embora não seja obrigatório, para fins de compatibilidade com as ferramentas atuais, devido ao fato de que algumas delas não seguem devidamente o que está definido nas normas, sugere-se que os valores dos campos Sujeito, Emissor e número serial deste novo certificado sejam semelhantes aos do certificado antigo.

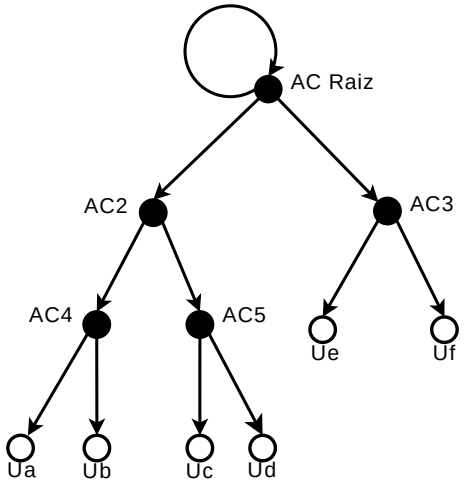

Figura 5.2: Estrutura de AC Hierárquica

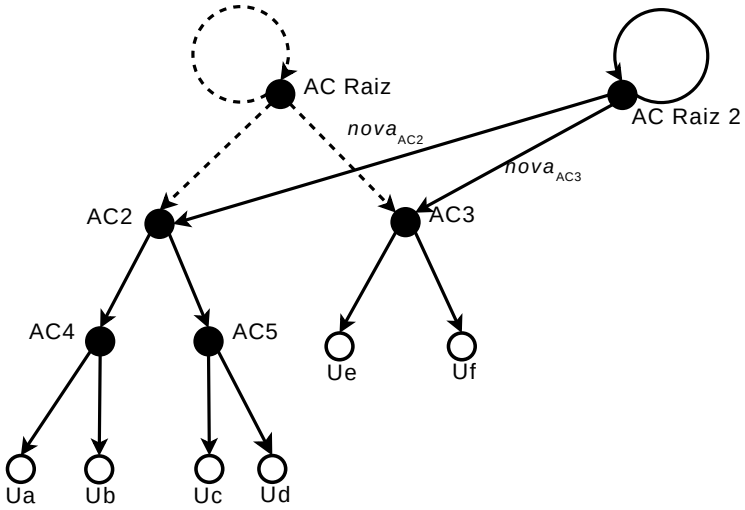

Figura 5.3: Emissão dos novos certificados das ACs intermediárias

Com a nova AC Raiz em funcionamento, o próximo passo é gerar requisições a partir de todos os certificados emitidos diretamente pela AC antiga. Este processo é bastante semelhante ao de atualização definido na seção 5.1.2, a única diferença é que estas requisições serão submetidas a uma outra AC ao invés da mesma, neste caso, a nova

AC Raiz. Este passo se faz necessário para que todas as ACs de nível imediatamente inferior ao da AC Raiz antiga possam se vincular a nova AC Raiz.

Geradas as requisições, a nova AC Raiz deve emitir os certificados referentes as requisições criadas. Estes novos certificados de autoridades certificadoras intermediárias devem obrigatoriamente ter os mesmos valores do campo Sujeito e a mesma chave pública de seus respectivos certificados antigos. Com isto, estes novos certificados permitem o estabelecimento do caminho de certificação até a nova AC Raiz. Na figura 5.3 os novos certificados são apresentados como $nova_{AC2}$ e $nova_{AC3}$

Devido ao fato dos novos certificados das Autoridades Certificadoras subordinadas serem semelhantes aos antigos e possuírem o mesmo par de chaves, todos os certificados emitidos em níveis hierárquicos inferiores aos certificados reemitidos não sofrerão implicações, e poderão construir caminhos de certificação válidos até a nova AC Raiz sem a necessidade de nenhum recurso adicional além do uso dos certificados digitais.

Os períodos de validade dos novos certificados emitidos neste processo não apresentam restrições além daquelas sob as quais qualquer certificado é submetido, como por exemplo, restrições de validade para determinados tamanhos de chaves, algoritmos, etc.

Outro passo de fundamental importância para que este procedimento seja bem sucedido é a publicação e divulgação do novo certificado da AC Raiz de forma que todos que necessitem obter este novo certificado possam fazê-lo. Esta publicação pode ser realizada através dos repositórios da AC e preferencialmente todos os subscritores desta ICP devem ser notificados para que obtenham os novos certificados.

As novas ACs geradas no processo podem desempenhar o mesmo papel das ACs anteriores (emissão e revogação de certificados, criação de LCRs, etc). Os certificados antigos não precisam ser revogados, e podem ser mantidos válidos até que expirem. A Figura 5.4 apresenta a nova estrutura após toda a realização do processo.

Este novo método atende a todos os requisitos listados, pois:

- é totalmente compatível com as normas atuais;
- não tem a necessidade do uso da antiga chave privada;
- permite o restabelecimento do funcionamento da ICP de forma rápida, pois é necessária apenas a reemissão dos certificados da AC Raiz e das ACs cujos certificados

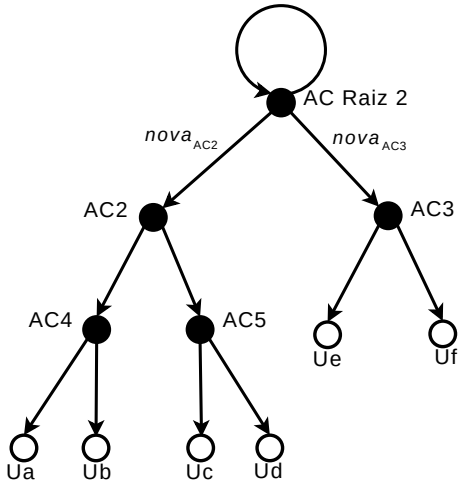

Figura 5.4: Nova estrutura após a realização do novo método

foram emitidos pela AC Raiz, o que raramente representa um número alto de reemissões. Além disso, por manter os mesmos atributos nos certificados, permite a emissão dos novos certificados de forma automática e segura, aumentando significativamente a velocidade do processo;

- não utiliza nenhum estrutura nova, o restabelecimento da confiança se dá apenas através da capacidade de construção dos caminhos de certificação dos certificados.

Analisando a redução do impacto em relação à reemissão de todos os certificados, pode-se dizer que este foi mínimo, já que a necessidade de reemissão de certificados se restringiu a um único nível na cadeia de certificação. Dado n, como o número de certificados de ACs intermediárias emitidos pela AC Raiz e x o número total de certificados emitidos a partir de cada uma dessas ACs, a necessidade de reemitir certificados é reduzido de $n * x$ para apenas n, tornando o custo bastante reduzido.

Já no caso da aplicação desta técnica em uma AC intermediária, o impacto pode ser maior. Se esta AC intermediária emite certificados apenas para ACs, a redução de impacto se aplica de maneira semelhante à apresentada acima, porém se esta AC emite certificados para entidades finais, o custo é igual à reemissão de todos os certificados emitidos.

5.2.1.1 Construção do caminho de certificação para o novo certificado

Conforme discutido anteriormente, a forma como o caminho de certificação para o novo certificado é construído depende das informações contidas nos certificados existentes neste caminho. Portanto, a construção depende dos valores das extensões e dos valores do campo Sujeito do certificado.

Encadeamento por nome

A partir do restabelecimento da ICP, a publicação dos novos certificados nos repositórios e a obtenção destes novos certificados pelas entidades que desejam fazer as construções dos caminhos, a construção do caminho de certificação para o novo certificado é feita automaticamente, ou seja, através do método de encadeamento por nome apresentado na seção 3.6.1.1.

Isto é possível pelo fato dos certificados das ACs cujos certificados foram emitidos pela AC Raiz antiga terem também sido reemitidos pela nova AC Raiz.

Encadeamento por identificador de chave

A construção de caminho de certificação utilizando este método também é realizada corretamente. Mesmo que a extensão AKID contenha apenas o valor do campo *keyIdentifier* ou contiver também os valores de *authorityCertIssuer* e *authoritySerialNumber*, as implementações da construção de caminho de certificação que estiverem de acordo com as definições do padrão x.509 montarão o caminho de certificação corretamente até o novo certificado.

Partindo do certificado de entidade final até o ponto de confiança, a comparação é feita conforme descrito na seção 3.6.1.2. Com isso, serão encontrados dois caminhos candidatos, um deles apontando para o certificado antigo e outro para o novo. Se a extensão AKID do certificado de nível imediatamente inferior ao certificado alterado contiver apenas o campo *keyIdentifier* definido, o caminho de certificação iniciará a fase de validação do caminho a partir do certificado novo, e após a validação, aceitará este caminho como válido. Se o AKID do contiver os campos *authorityCertIssuer* e *authorityCertSerialNumber* definidos, estes valores coincidirão apenas com o certificado antigo, fazendo com que seja dada preferência para este caminho e a etapa de validação seja inicialmente realizada através deste. Porém, se o ponto de confiança de quem verifica

for a nova AC Raiz, a construção até o antigo certificado não chegará ao ponto de confiança desejado e consequentemente a validação através do segundo caminho será realizada e aceita.

5.2.2 Com chave privada disponível

Quando se tem a chave privada disponível e deseja-se realizar a troca da chave privada, existem dois casos que podem ser diferenciados. Um onde existe a disponibilidade da chave privada e não existem quaisquer restrições sobre seu uso, sejam elas restrições de cópia, de confiança, etc. Outro caso é quando existem restrições sobre o uso da chave, o que implica em uma análise mais detalhada sobre qual procedimento deve ser realizado.

5.2.2.1 Com restrições sobre a chave

A idéia de restrições sobre uma chave privada é muito ampla, e deve ser analisada com extrema precisão pelo operador de uma AC antes que se decida qual procedimento deve ser seguido. As restrições mais comuns sobre uma chave privada são:

- obsolência de tecnologia;
- grau de proteção da chave;
- possibilidade da realização de cópias de segurança;
- confiabilidade nos equipamentos que armazenam a chave;
- confiabilidade no software que utiliza a chave;
- políticas.

Portanto, cabe ao operador da AC analisar quais restrições existem sobre a chave, e conseqüentemente definir qual procedimento utilizar. Apesar das possíveis restrições serem amplas, podemos generaliza-lás em duas categorias: (I) críticas, onde não se deseja mais utilizar e confiar na chave antiga; e (II) não críticas, onde embora existam restrições, elas não implicam em necessidade de destruição da chave, podendo esta, inclusive ser utilizada durante o procedimento de criação do novo ambiente seguro, e do estabelecimento da nova Autoridade Certificadora.

No caso das restrições sobre a chave não serem críticas, pode-se utilizar o CMP, CTL, ou o novo método descrito na seção 5.2.1. Isto porque se decidiu que a chave antiga pode ser utilizada sem grandes implicações, e este método faz a mudança no ponto de confiança com um impacto bastante reduzido, com a necessidade apenas da emissão do novo certificado e par de chaves, e mais dois certificados de transição. Além disso, a chave privada antiga será utilizada apenas para assinar o certificado de transição, depois disso ela não será mais necessária.

Se as restrições sobre a chave forem consideradas críticas, e consequentemente não se desejar utilizá-la novamente, a maneira mais adequada de se proceder é utilizar o novo método definido na seção 5.2.1. A utilização deste método é considerada adequada pelo fato de não utilizar em nenhum momento a chave privada antiga, sendo que esta pode ser destruída antes mesmo da utilização do método. Além disso, o novo método embora tenha um impacto um pouco maior sobre a ICP, é completamente transparente para todas as entidades da ICP a partir de seu segundo nível hierárquico.

5.2.2.2 Sem restrições sobre a chave

Caso a chave privada esteja disponível e não existam quaisquer restrições quanto a seu uso e confiabilidade, pode-se considerar que a chave privada está protegida e pode ser utilizada sem restrições. Com isto, o procedimento de troca a ser adotado pode ser o CMP, CTL ou o novo método, já que estes permitem a utilização da chave privada antiga e apresentam um baixo grau de impacto sobre a ICP.

5.3 Conclusão

O presente capítulo tratou, de forma detalhada e aplicada em situações reais de uma ICP, as diferentes formas de lidar com eventos que impliquem na necessidade de realizar qualquer operação de substituição de chaves e certificados de uma AC. As operações de substituição de certificados foram detalhadas de maneira mais precisa, e com um enfoque prático. As operações de substituição de chaves criptográficas de uma AC foram tratadas de maneira mais abrangente do que os métodos atualmente existentes na literatura, e com isto, situações críticas podem ser tratadas de maneira mais ágil e precisa.

Capítulo 6

Topologias Dinâmicas

Além das aplicações já apresentadas anteriormente, a análise e a implementação destes métodos permitiu que novas aplicações fossem desenvolvidas. Uma delas é o que podemos chamar de topologias dinâmicas.

As topologias dinâmicas são casos particulares dos métodos de troca do par de chaves de ACs e renovação de certificados. Este capítulo descreve quatro desses casos. Inicialmente será apresentada a união de ICPs, onde duas ou mais ICPs já estabelecidas se unem, subordinando-se a uma nova AC Raiz. A segunda aplicação é a subordinação de ICPs, que trata o caso de uma ICP pré-existente passar a ser subordinada de outra. Na seqüência, é apresentado um método de emancipação de ACs, fazendo com que uma AC se torne independente da ICP à qual ela era vinculada. Finalmente será tratada a migração de ACs, onde uma AC pode trocar dinamicamente de ICP sob a qual ela é subordinada.

Para os casos que serão apresentados, com exceção do caso de emancipação de ACs, algumas restrições devem ser observadas:

- o conteúdo da extensão *basic constraints* dos certificados de ACs a serem emitidos deve sempre estar dentro das limitações impostas pela AC Raiz;
- todos os certificados e ACs criadas devem respeitar as políticas e práticas de certificação definidas pela AC Raiz;
- todas as restrições políticas das ACs devem estar conformes umas com as outras e não poderão invalidar a aceitação dos certificados de outras ACs dentro da mesma ICP.

6.1 União de ICPs

O mecanismo de união de ACs permite unir duas ou mais ICPs já estabelecidas em uma nova hierarquia comum sem a necessidade do estabelecimento de certificação cruzada ou em ponte entre elas. Uma de suas vantagens é evitar algumas das desvantagens referentes a estas arquiteturas, como o surgimento de não determinismos e dificuldades na construção no caminho de certificação.

Para estabelecer a união entre duas ICPs, o procedimento a ser realizado é o seguinte:

a) cria-se um novo par de chaves para a nova AC Raiz;

b) emite-se um novo certificado de AC Raiz (auto-assinado) utilizando o novo par de chaves;

c) para cada AC Raiz das antigas ICPs, emite-se um novo certificado, contendo o mesmo valor do campo *Subject* e a mesma chave pública do anterior, assinado pela nova AC Raiz;

d) publicam-se os novos certificados nos repositórios e de outras possíveis maneiras.

A Figura 6.1 apresenta duas ICPs distintas (ICP I e ICP II) antes da realização da união entre elas e a Figura 6.2 apresenta as estruturas em seu estado final. As setas tracejadas representam os antigos certificados das ACs, que não estão mais em uso.

A principal vantagem deste modelo em relação a arquiteturas de certificação cruzada ou ponte é a redução da complexidade na construção e verificação do caminho de certificação e um menor número de certificados a serem emitidos. Quanto maior o número de ACs envolvidas, maior a redução da complexidade em relação às outras arquiteturas. Como resultado da criação desta nova AC Raiz para intermediar as relações de confiança, dado n como o número de ACs, a redução cai de $(n^2 - n)$ certificados para certificação cruzada e $2n$ para certificação em ponte para $n + 1$ certificados neste modelo. Além disso, por se tratar de uma estrutura hierárquica, a construção do caminho de certificação será determinística, ao contrário das outras arquiteturas, tornando a complexidade da construção do caminho de certificação bastante reduzida.

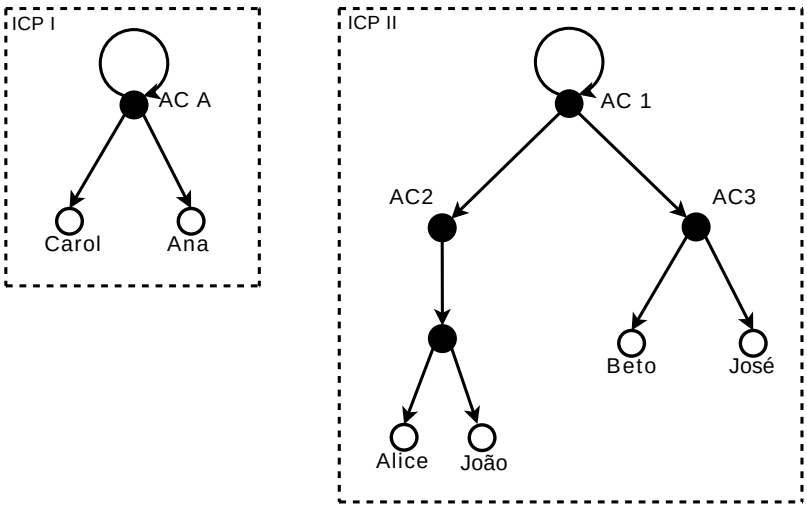

Figura 6.1: Duas ICPs distintas antes da realização da União

O período de validade dos certificados emitidos durante este processo se inicia no momento em que são emitidos e se encerra em uma data que deve ser superior à data de expiração do último certificado emitido por cada AC. Os certificados antigos podem ser mantidos válidos até que expirem, e as ACs cujos certificados foram reemitidos podem desempenhar as mesmas funções que realizavam anteriormente sem nenhuma restrição.

6.1.1 Construção do caminho de certificação para o novo certificado

O método de União de ICPs possui várias semelhanças com método de substituição de chaves apresentado na seção 5.2.1, e devido a isto, o mesmo ocorre com a construção do caminho de certificação.

Encadeamento por nome

A partir criação da nova AC Raiz e a publicação dos novos certificados das ACs nos repositórios, a construção do caminho de certificação para o novo certificado é feita automaticamente, ou seja, através do método de encadeamento por nome apresentado na seção 3.6.1.1.

Isto ocorre devido ao fato de que os certificados que anteriormente eram de AC Raiz, foram reemitidos e o campo Emissor destes novos certificados aponta para a nova AC Raiz.

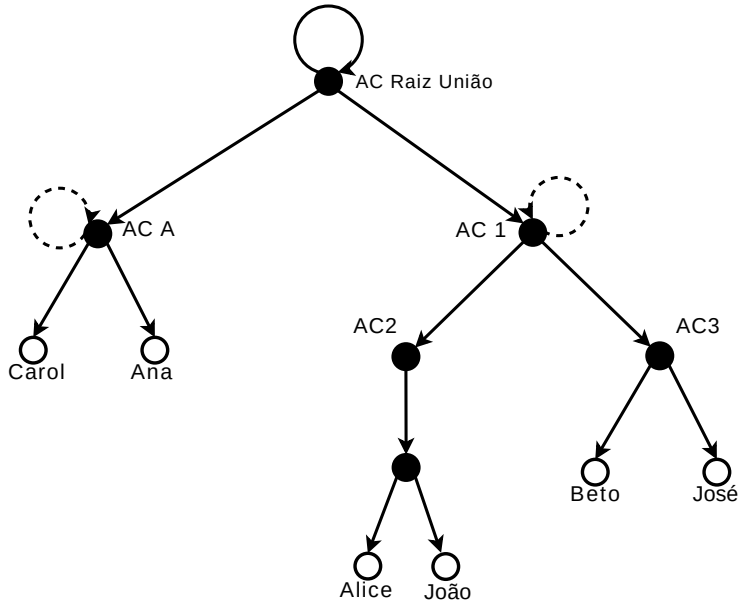

Figura 6.2: Estrutura final após a União entre ICPs

Encadeamento por identificador de chave

A construção de caminho de certificação neste caso também é realizada corretamente. Todas as ferramentas que possuírem implementações para a construção de caminho de certificação que estiverem de acordo com as definições do padrão x.509 montarão o caminho de certificação corretamente utilizando os novos certificados.

Partindo do certificado de entidade final até o ponto de confiança, a comparação é feita conforme descrito na seção 3.6.1.2. Com isso, serão encontrados dois caminhos candidatos, um deles apontando para o certificado antigo (antiga AC Raiz), e consequentemente possuindo um certificado a menos no caminho de certificação, e outro apontando para o certificado da nova AC Raiz. Se a extensão AKID do certificado de nível imediatamente inferior ao certificado alterado contiver apenas o campo *keyIdentifier* definido, o caminho de certificação iniciará a fase de validação do caminho a partir do certificado novo, e após a validação, aceitará este caminho como válido. No caso da extensão AKID conter também os campos *authorityCertIssuer* e *authorityCertSerialNumber* definidos, este valores coincidirão apenas com o certificado antigo, e com isso será dada preferência ao caminho que inclui este certificado. Porém se este caminho não contiver o ponto de confiança de quem o verifica, a validação através do segundo caminho será realizada, e consequentemente aceita.

6.2 Subordinação de ICPs

A subordinação de ACs é mais um derivação dos métodos apresentados. Este método consiste na inclusão de uma ou mais ICPs já estabelecidas sob uma outra ICP, de modo que se constitua uma hierarquia entre elas e conseqüentemente, se estabeleça um ponto de confiança único e pré-existente. A AC raiz de cada ICP que se subordinará à outra, será chamada de AC Raiz Secundária, e a AC Raiz da ICP que incorporará as outras ICPs sob sua topologia, será chamada de AC Raiz Principal.

A principal diferença deste método em relação ao de União de ACs é que neste método, uma das ICPs permanecerá com o seu ponto de confiança original, ou seja, manterá sua AC Raiz. Já as outras ICPs envolvidas no processo terão um nível hierárquico acrescentado, e terão como ponto de confiança a AC Raiz Principal.

Para subordinar uma ICP à outra, os seguintes passos devem ser seguidos:

- a partir do certificado da AC Raiz Secundária, gera-se uma requisição de certificado contendo o mesmo valor do campo *Subject* e a mesma chave pública;
- a AC Raiz principal emite um novo certificado a partir da requisição da AC Raiz secundária, subordinando-a a sua estrutura.
- publicam-se os novos certificados nos repositórios e de outras possíveis maneiras;

A Figura 6.2, apresentada no método de União de ICPs como exemplo de estrutura inicial, será considerada também como ponto de partida antes da realização da subordinação de ACs. Após a realização do procedimento, a estrutura apresentada terá seu estado final de acordo com o que está demonstrado na Figura 6.3. No exemplo da figura, a AC A se subordina à AC 1 e passa a fazer parte de sua hierarquia.

Este método mostra-se importante na redução de custos caso uma ICP já estabelecida deseje filiar-se à outra, de forma a possuírem um ponto de confiança comum. A sua utilização evita a necessidade de reemissão de todos os certificados da ICP Secundária para que estes façam parte da ICP Principal. Além disso, torna possível que certificados de ICPs cujo ponto de confiança não seja muito difundido e aceito, possam ser aceitos de maneira mais ampla a partir do momento que sua ICP se subordinar a uma outra de maior aceitação e popularidade.

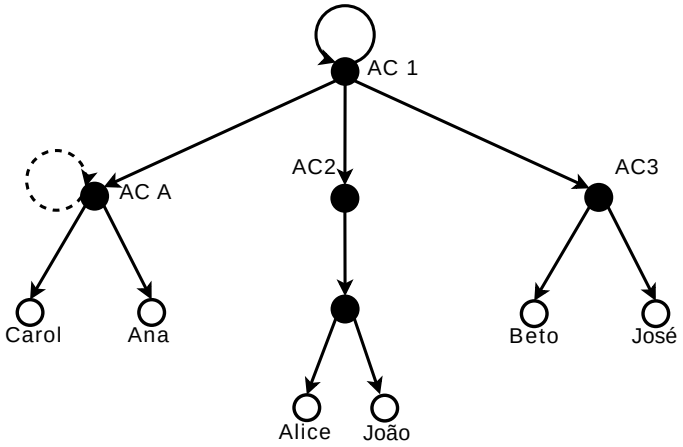

Figura 6.3: Estrutura final após a subordinação de ICPs

O período de validade do certificado emitido durante este processo se inicia no momento em que o certificado é emitido, e se encerra em uma data que deve ser superior à data de expiração do último certificado emitido por esta AC e inferior a da AC que o emitiu. Os certificados antigos podem ser mantidos válidos até que expirem, e as ACs cujos certificados foram reemitidos podem desempenhar as mesmas funções que realizavam anteriormente desde que as políticas da nova ICP permitam.

6.2.1 Construção do caminho de certificação para o novo certificado

Assim como na União de ICPs, a construção do caminho de certificação se dá de maneira semelhante ao que ocorre no caso apresentado na seção 5.2.1, que trata a substituição de chaves de ACs sem a chave privada antiga disponível.

Encadeamento por nome

A partir criação da nova AC Raiz e da publicação dos novos certificados das ACs nos repositórios, a construção do caminho de certificação para o novo certificado é feita automaticamente, pelo fato de que o certificado que anteriormente representava uma AC raiz foi reemitido e seu campo Emissor passou a apontar para a AC Raiz Principal.

Encadeamento por identificador de chave

Através do encadeamento por identificador de chaves, a construção de caminho de certificação também é realizada corretamente. Todas as implementações de construção de caminho de certificação que estiverem de acordo com as normas montarão o caminho de certificação corretamente até o novo certificado.

Durante a construção do caminho de certificação serão encontrados inicialmente dois caminhos candidatos, um deles apontando para a AC Raiz Secundária, e outro levando para a AC Raiz Principal. Se a extensão AKID do certificado de nível imediatamente inferior ao da AC Raiz Secundária contiver apenas o campo *keyIdentifier*, o caminho de certificação iniciará a fase de validação do caminho a partir do novo certificado, e após a validação, aceitará este caminho. No caso da extensão AKID conter os campos *authorityCertIssuer* e *authorityCertSerialNumber*, será dada preferência para o caminho antigo (AC Secundária). Porém, se o ponto de confiança da entidade que está realizando a verificação, for a nova AC Raiz, a construção do caminho de certificação só será completa ao utilizar o caminho que contém a nova AC Raiz.

6.3 Emancipação de ACs

A emancipação de uma AC é uma maneira de separar uma AC, e toda a estrutura existente a partir dela, da ICP a qual ela pertence. Esta aplicação pode ser utilizada em vários casos, como por exemplo no desvinculamento de um setor de uma organização, supondo que este deseje manter toda a estrutura de sua AC.

Este caso representa uma situação oposta à da subordinação de ACs, já que ao invés de substituir um certificado de AC Raiz por um de AC Intermediária, este método substitui um certificado de AC Intermediária por um de AC Raiz.

Para emancipar uma AC, o procedimento é o seguinte:

- A AC Subordinada que deseja se emancipar emite um certificado auto-assinado contendo o mesmo valor do campo *Subject* e a mesma chave pública do anterior;
- o certificado antigo é revogado pela AC Raiz;
- publicam-se os novos certificados nos repositórios e de outras possíveis maneiras;

A figura 6.4 apresenta um exemplo de ICP antes da remoção do vínculo. O procedimento de emancipação é realizado na AC 2, e o resultado pode ser observado na figura 6.5, onde existem duas ICPs, a ICP I, que agora não possui a AC 2 em sua topologia, e a ICP Removida, que possui como ponto de confiança a AC 2, recém emancipada.

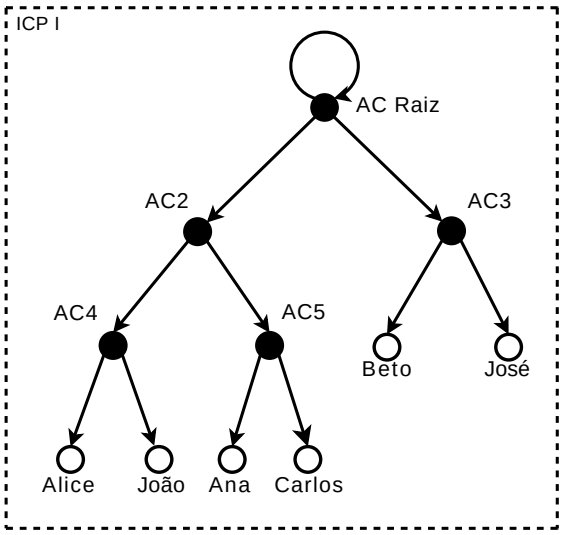

Figura 6.4: ICP inicial antes da emancipação

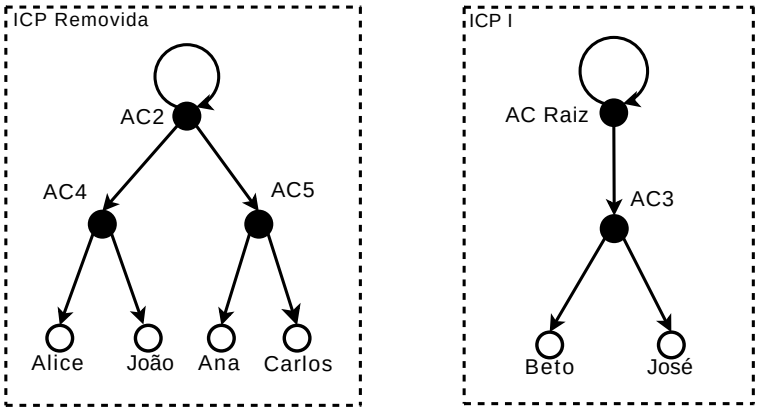

Figura 6.5: ICPs resultantes do processo de emancipação

A utilização deste método pode reduzir significativamente os custos de uma ICP já estabelecida que necessite remover seu vínculo com a ICP à qual ela pertence. Esta redução de custos se dá pelo fato de não haver a necessidade de reemissão de um grande número de certificados, e nem mesmo requerer a criação de um novo par de chaves. Apenas um certificado precisa ser reemitido durante a realização de todo este processo. Outra vantagem resultante da emancipação é que, por ser tornar o ponto de confiança de

sua própria ICP, a AC emancipada pode ter maior independência e flexibilidade, ficando restrita apenas a sua própria política.

O período de validade do certificado emitido se inicia no momento em que o certificado é emitido e se encerra em uma data que deve ser superior à data de expiração do último certificado emitido por esta AC antes de sua emancipação.

O certificado antigo, pertencente a ICP de origem, deve ser revogado, pois a ICP de origem não terá nenhuma relação de confiança com a nova ICP, e portanto não pode aceitar como válido em sua topologia, o certificado antigo da AC Emancipada.

6.3.1 Construção do caminho de certificação para o novo certificado

Na emancipação de uma AC, a construção do caminho de certificação funciona de maneira semelhante aos métodos anteriores, porém possui com o diferencial que está no fato de que o novo caminho de certificação passa a ser menor do que o caminho anterior.

Encadeamento por nome

A partir reemissão do certificado auto-assinado da nova AC Raiz e a publicação deste nos repositórios, a construção do caminho de certificação para a nova ICP é feita automaticamente, ou seja, através do método de encadeamento por nome apresentado na seção 3.6.1.1.

Isto ocorre pelo fato de que o certificado que anteriormente representava uma AC Intermediária, foi reemitido e transformou-se em um certificado de AC Raiz, onde o campo Emissor deste é igual ao seu campo Sujeito.

Encadeamento por identificador de chave

A construção do caminho de certificação utilizando este método também é realizada corretamente. Mesmo que a extensão AKID contenha apenas o valor do campo *keyIdentifier* ou também contenha os valores de *authorityCertIssuer* e *authoritySerialNumber*, as implementações da construção de caminho de certificação que estiverem de acordo com as definições do padrão x.509 montarão o caminho de certificação corretamente utilizando a nova ICP.

Partindo do certificado de entidade final até o ponto de confiança, a comparação é feita conforme descrito na seção 3.6.1.2. Com isso, serão encontrados dois caminhos candidatos, um deles passando pela AC Intermediária Emancipada e apontando para o certificado da AC Raiz da antiga ICP e outro para o novo certificado. Se a extensão AKID do certificado de nível imediatamente inferior ao certificado alterado contiver apenas o campo *keyIdentifier* definido, o caminho de certificação iniciará a fase de validação do caminho a partir do certificado novo, e após a validação, aceitará este caminho como válido. Se o AKID do contiver os campos *authorityCertIssuer* e *authorityCertSerialNumber* definidos, estes valores coincidirão apenas com o certificado antigo, fazendo com que seja dada preferência para este caminho e a etapa de validação seja inicialmente realizada através deste. Porém, este caminho não será aceito na etapa de validação, pois o certificado da AC Intermediária Emancipada estará revogado. Com a rejeição do caminho, a validação se dará utilizando o próximo caminho candidato, que remete à nova ICP, e consequentemente será validado.

6.4 Migração de ACs

A migração de ACs trata-se da aplicação da emancipação de uma AC sem a emissão de um novo certificado auto-assinado e posteriormente a realização do método de subordinação de ACs. Com isto, este método pode agregar as vantagens apresentadas pelos dois métodos dos quais ele deriva.

Para realizar a migração de uma ICP, o procedimento é o seguinte:

- A AC Subordinada que deseja migrar de ICP deve criar uma nova requisição contendo o mesmo valor do campo *Subject* e a mesma chave pública de seu certificado;
- A AC da ICP de destino emite um novo certificado a partir da requisição da AC requisitante, subordinando-a a sua estrutura;
- o certificado antigo da AC Requisitante é revogado pela AC que o emitiu;
- publicam-se os novos certificados nos repositórios e de outras possíveis maneiras;

A figura 6.6 apresenta um exemplo de duas ICPs antes da migração da AC 3, que se desvincula da ICP I e se subordina à ICP II. Após a realização do procedi-

mento de migração, o resultado pode ser observado na figura 6.7, onde a ICP I não conta mais com a AC 3, e a ICP II tem a AC 3 incorporada à sua topologia.

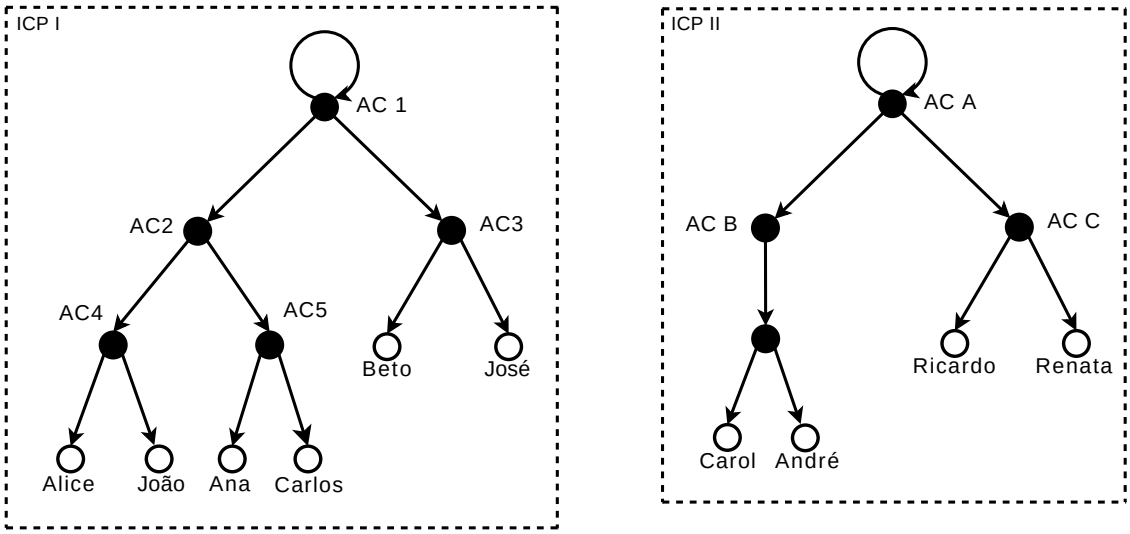

Figura 6.6: Duas ICPs antes da migração de ACs

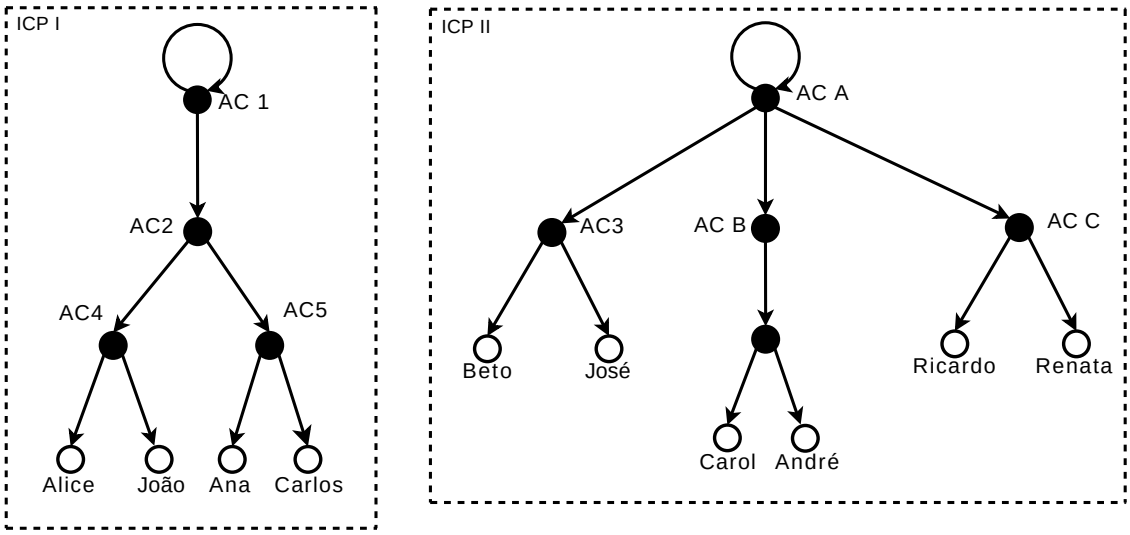

Figura 6.7: Nova topologia das ICPs após a migração da AC 3

A utilização deste método agrega vantagens existentes aos métodos de subordinação de ICPs e de emancipação de ACs, tornando possível, por exemplo, que uma AC remova seu vínculo com uma ICP pouco aceita, e sem que seja necessário reemitir seus certificados, passe a fazer parte de uma ICP de maior popularidade e aceitação. Com isto, pode-se observar que para migrar uma AC, os custos são baixos, poucos certificados precisam ser emitidos e todas as vantagens advindas da subordinação de ACs são

existentes também neste caso.

O período de validade do certificado emitido durante este processo se inicia no momento de sua emissão e se encerra em uma data que deve ser superior à data de expiração do último certificado emitido por esta AC e inferior à da AC que o emitiu.

De forma semelhante ao que ocorre na emancipação de ACs, o certificado antigo da AC pertencente à ICP de origem deve ser revogado, pois esta ICP não terá mais responsabilidade e nenhuma relação de confiança com a AC que agora pertence a uma outra ICP. Portanto, a ICP de origem não aceitará como válido em sua topologia o certificado antigo da AC que realizou a migração.

6.4.1 Construção do caminho de certificação para o novo certificado

Na migração de ACs, a construção do caminho de certificação se dá de maneira semelhante ao que ocorre no caso de Emancipação de ACs.

Encadeamento por nome

Após a emissão e publicação do novo certificado pela AC que o emitiu na ICP de destino, a construção do caminho de certificação para a nova ICP é feita automaticamente, ou seja, através do método de encadeamento por nome apresentado na seção 3.6.1.1. Isto ocorre pelo fato de que o certificado que anteriormente pertencia a uma ICP foi reemitido e transformou-se em um certificado vinculado à outra ICP.

Encadeamento por identificador de chave

A construção do caminho de certificação utilizando este método também é realizada corretamente. Se a extensão AKID contiver apenas o valor do campo *keyIdentifier* ou também os valores de *authorityCertIssuer* e *authoritySerialNumber*, as implementações da construção de caminho de certificação que estiverem de acordo com as definições do padrão x.509 montarão o caminho de certificação corretamente até o novo certificado.

Partindo do certificado de entidade final até o ponto de confiança, a comparação é feita conforme descrito na seção 3.6.1.2. Com isso, serão encontrados dois caminhos candidatos, um deles apontando para os certificados da ICP antiga e outro para a nova. Se a extensão AKID do certificado de nível imediatamente inferior ao certificado

alterado contiver apenas o campo *keyIdentifier* definido, o caminho de certificação iniciará a fase de validação do caminho a partir do certificado novo, e após a validação, aceitará este caminho como válido. Se o AKID do contiver os campos *authorityCertIssuer* e *authorityCertSerialNumber* definidos, estes valores coincidirão apenas com o certificado antigo, fazendo com que seja dada preferência para este caminho e a etapa de validação seja inicialmente realizada através deste. Porém, este caminho não será aceito na etapa de validação, pois o certificado da AC Intermediária que realizou a migração estará revogado. Com a rejeição do primeiro caminho, a validação se dará utilizando o próximo, que remete à nova ICP, e consequentemente será validado.

6.5 Conclusão

Este capítulo descreveu em detalhes, métodos que permitem quem uma ICP realize, de maneira previsível e eficiente, alterações dinâmicas em sua topologia. Com isso, pode-se agregar diversas facilidades advindas da aplicação de cada um dos métodos. As situações apresentadas permitem a utilização de alternativas em relação aos métodos de estabelecimento de confiança entre ICPs conhecidos anteriormente e em alguns casos, melhorias em relação a custos, facilidade de construção do caminho de certificação e de estabelecimento do ponto de confiança.

Capítulo 7

Implementação e Validação

Esta etapa foi realizada juntamente ao trabalho de conclusão de curso de Jeandré Monteiro Sutil [37]. Para testes e validação das propostas apresentadas, foi escolhida a arquitetura Hierárquica por ser a de maior uso atualmente e também por ser uma estrutura que permite fácil visualização dos resultados em outras arquiteturas, como AC Única, Teia, Certificação Cruzada e Ponte.

Foram criadas diversas estruturas, que incluem desde ICPs mais simples até ICPs com topologias mais complexas, com diferentes quantidades de ACs intermediárias e níveis de cadeia. Para facilitar o entendimento dos procedimentos, as topologias das ICPs serão divididas em subgrupos chamados níveis, onde a AC Raiz é o nível 0, as ACs cujos certificados foram emitidos pela AC Raiz serão nível 1, e assim por diante. Os certificados emitidos para entidades finais, ou seja, certificados que não são de Autoridades Certificadoras, serão identificados por certificados de entidades finais.

Para cada Autoridade Certificadora, foram emitidos milhares de certificados, a fim de que a simulação do ambiente fosse mais fiel a um ambiente real. Além disso, vale ressaltar que nas simulações foram emitidos certificados utilizando as extensões *Authority Key Identifier* e *Subject Key Identifier*, e também certificados que não utilizaram estas extensões, forçando desta forma a construção estritamente por nomes.

Para os certificados que utilizaram a extensão *Authority Key Identifier*, foram feitos testes com possíveis combinações desta extensão, ou seja, definindo apenas o valor do atributo *keyIdentifier*, que chamaremos de AKID Básico, e definindo os três atributos possíveis, *keyIdentifier*, *authorityCertIssuer* e *authoritySerialNumber*, que no decorrer desta seção chamaremos de *AKID Completo*.

A montagem do caminho de certificação é realizada utilizando-se um certificado de entidade final como ponto de partida e realizando a troca da Autoridade Certificadora Raiz da ICP a qual o certificado pertence.

Com o ambiente de testes pronto, foram escolhidas as seguintes ferramentas para testar a portabilidade e compatibilidade dos métodos aos sistemas existentes atualmente:

Navegador Mozilla Firefox versão 2.0 – este navegador foi escolhido por ter seu uso em crescimento atualmente, apresentar uma biblioteca criptográfica própria, chamada NSS [38], tornando-se uma importante referência na avaliação de aplicabilidade dos métodos. Os testes realizados utilizando esta ferramenta foram feitos tanto em ambiente Windows (XP *Professional*) quanto Linux (*kernel* 2.6);

Navegador Internet Explorer versão 6.0 – este navegador foi escolhido por ser o mais utilizada atualmente, ser integrado com o repositório de chaves de certificados do sistema operacional Windows e utilizar bibliotecas da microsoft como a CryptoAPI [39]. Os testes realizados utilizando esta ferramenta foram feitos em ambiente Windows (XP *Professional*);

OpenSSL versão 0.9.8 – este conjunto de ferramentas e biblioteca foi escolhido por ser o mais utilizando em ambientes que utilizam software livre, ter grande aceitação e possuir uma biblioteca bastante abrangente para implementados de ICP [40]. Os testes realizados utilizando esta ferramenta foram feitos em ambiente Linux (*kernel* 2.6);

Nas seções seguintes serão apresentados os resultados dos testes e validações realizadas utilizando todos os métodos apresentados no decorrer do capítulo 5 seguindo as condições definidas acima. Na seção 7.1 serão apresentados os resultados referentes aos testes sobre substituição dos certificados nas ACs. Na seção 7.2 serão apresentados os resultados referentes aos testes sobre substituição de chaves criptográficas das ACs.

7.1 Substituição do Certificado

Nesta seção, os testes foram divididos em duas categorias: os de alteração do certificado, onde o certificado foi substituído e o novo certificado possuía atributos diferentes do anterior; e os de renovação do certificado, onde o novo certificado possui dados semelhantes aos do certificado anterior.

7.1.1 Alteração do Certificado

Conforme definido na seção 5.1.1, o processo de alteração do Certificado implica na modificação em alguns de seus atributos. Além disso, pode-se dividir a alteração dos atributos em duas categorias: críticos e não críticos. A alteração de atributos críticos implica em problemas de montagem ou validação do caminho de certificação, já a modificação de atributos não críticos não geram tais problemas.

De acordo as definições da seção 3.6, pode-se concluir que são críticos os seguintes campos:

- sujeito;
- extensão *Basic Constraints*;
- quaisquer extensões que impliquem em alterações nas restrições de políticas.

Os demais campos não serão considerados críticos.

A partir disto foram criados dois cenários de testes: (I) um onde não foram realizadas alterações em atributos críticos e outro (II) onde valores do campo sujeito foram modificados, e para cada um deles foram utilizados os critérios definidos no início deste capítulo. Definidos os cenários, o seguinte procedimento foi realizado:

a) a estrutura inicial da ICP é criada;
b) o caminho de certificação é verificado;
c) o certificado da Autoridade Certificadora Raiz é modificado seguindo o método definido na seção 5.1.1;
d) incorpora-se o novo certificado a lista de possíveis certificados do caminho certificação;

e) o caminho de certificação é novamente verificado;

f) se necessário, remove-se o certificado antigo da AC Raiz da lista;

g) o caminho de certificação é novamente verificado.

7.1.1.1 Resultados

Internet Explorer

Para o cenário I, a construção do caminho de certificação por nomes foi realizada corretamente, ou seja, a partir do momento em que o novo certificado foi incorporado à lista, o caminho de certificação foi automaticamente construído apontando para o novo certificado. Com o uso do AKID básico a construção do caminho de certificação também foi realizada corretamente, com comportamento semelhante à construção por nomes. Já com o uso do AKID completo, o caminho de certificação inicialmente apontou para o certificado antigo, já que conforme o que define o padrão X.509, os valores contidos nos campos *authorityCertIssuer* e *authoritySerialNumber* foram utilizados para definir preferência ao certificado antigo devido ao número serial. Porém, com a realização do passo f do procedimento, o caminho foi construído automaticamente até o novo certificado, mostrando total aderência ao definido nas normas.

Para o cenário II, em todos os casos, o caminho de certificação não foi construído até o novo certificado, mostrando que embora alguns campos, como por exemplo o número serial do certificado, possam ser alterados sem problemas, outros, como o Sujeito, não podem sofrer alteração.

Mozilla Firefox

No cenário I, assim como no Internet Explorer, a construção do caminho de certificação por nomes foi realizada corretamente a partir do momento em que o novo certificado foi incorporado a lista. Com o uso do AKID básico a construção do caminho de certificação também foi realizada corretamente, com o mesmo comportamento da construção por nomes. Com o AKID completo, foi selecionado inicialmente o caminho que levava ao certificado antigo, onde o campo serial era o mesmo contido na extensão AKID. Porém após a realização do passo f, o caminho não foi montado, indicando que a

montagem do caminho de certificação para o novo certificado não foi realizada corretamente.

A partir deste resultado, pode-se concluir que o navegador Mozilla Firefox mostrou um comportamento incorreto em relação às normas apresentadas na seção 3.6, já que ficou claro que ao invés de utilizar o valor dos atributos *authorityCertIssuer* e *authoritySerialNumber* para prover preferência na escolha, a implementação deste navegador considera obrigatório que seus valores sejam iguais aos dos certificados do caminho de certificação.

Para o cenário II, em todos os casos, o caminho de certificação não foi construído até o novo certificado, indicando que os atributos críticos não podem ser modificados.

OpenSSL

A montagem do caminho de certificação utilizando o OpenSSL não fornece informações detalhadas sobre a construção e validação do caminho de certificação, dificultando a análise de seus resultados. Porém em sua documentação, fica claro que a construção do caminho de certificação exige que cada campo da extensão *Authority Key Identifier* seja igual ao do certificado emissor para o sucesso da validação, e consequentemente, possui uma implementação diferente do que o especificado nas normas. Devido às limitações apresentadas, os resultados obtidos com o uso desta ferramenta não foram muito detalhados.

No cenário I, a construção do caminho de certificação por nomes foi realizada corretamente. Com o uso do AKID básico a construção do caminho de certificação também foi realizada corretamente, com comportamento semelhante à construção por nomes. Conforme o esperado, a construção utilizando o AKID completo não foi realizada corretamente.

Para o cenário II, em todos os casos, o caminho de certificação não foi construído corretamente.

7.1.1.2 Comparação dos resultados

No decorrer deste capítulo, em todas as tabelas apresentadas, o símbolo ✓ indicará sucesso, e o símbolo × indicará falha. A tabela 7.1 mostra uma síntese dos

resultados observados no cenário I:

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	✓	✓	✓
Mozilla Firefox	✓	✓	×
OpenSSL	✓	✓	×

Tabela 7.1: Resultados obtidos no procedimento de alteração do certificado da AC-Raiz no cenário I

A tabela 7.2 mostra uma síntese dos resultados observados no cenário II:

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	×	×	×
Mozilla Firefox	×	×	×
OpenSSL	×	×	×

Tabela 7.2: Resultados obtidos no procedimento de alteração do certificado da AC-Raiz no cenário II

7.1.2 Renovação do Certificado

Conforme definido na seção 5.1.2, o processo de renovação do certificado trata-se da maneira mais simples de realizar a substituição deste, já que não envolve alteração em nenhum de seus atributos com exceção de suas datas de validade.

Com isto, diferentemente do caso da alteração, apenas um cenário de testes se faz necessário, e para este, o seguinte procedimento foi realizado:

a) a estrutura inicial da ICP é criada;

b) o caminho de certificação é verificado;

c) o certificado da Autoridade Certificadora Raiz é renovado seguindo o método definido na seção 5.1.2;

d) incorpora-se o novo certificado à lista de possíveis certificados do caminho certificação;

e) o caminho de certificação é novamente verificado;

f) Se necessário, remove-se o certificado antigo da AC Raiz da lista;

g) os caminhos de certificação é novamente verificado.

7.1.2.1 Resultados

Internet Explorer

De maneira semelhante aos resultados encontrados na alteração de certificados para o cenário I, a construção do caminho de certificação por nomes e também no caso de uso do AKID básico foi realizada corretamente a partir do momento em que o novo certificado foi incorporado à lista. Com o uso do AKID completo, o comportamento também foi semelhante ao método de alteração no cenário I, ou seja, o caminho de certificação inicialmente apontou para o certificado antigo, e com a realização do passo f do procedimento, o caminho foi construído automaticamente até o novo certificado, mostrando total aderência ao definido nas normas.

Mozilla Firefox

Nos casos de construção do caminho de certificação por nomes e por AKID básico, a montagem foi realizada corretamente. Com o uso do AKID completo, o caminho escolhido apontava para o certificado antigo, onde o campo serial era o mesmo contido na extensão AKID. Após a realização do passo f, o caminho não foi montado, apresentando o mesmo problema já indicado nos testes de alteração de certificado.

Novamente pode-se concluir que o navegador Mozilla Firefox mostrou um comportamento incorreto em relação às normas apresentadas na seção 3.6 pelo mesmos motivos citados anteriormente, ou seja, ao invés de utilizar o valor dos atributos *authorityCertIssuer* e *authoritySerialNumber* para prover preferência na escolha, a implementação deste navegador considera obrigatório que seus valores sejam iguais aos dos certificados do caminho de certificação.

OpenSSL

Conforme o que foi descrito anteriormente, o comportamento esperado para os testes utilizando o OpenSSL deve refletir a não aderência de sua implementação às normas. Com isto, a construção do caminho de certificação por nomes e por AKID básico foi realizada corretamente. Conforme o esperado, a construção utilizando o AKID completo não foi realizada corretamente.

7.1.2.2 Comparação dos resultados

A tabela 7.3 mostra uma síntese dos resultados observados nos testes:

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	✓	✓	✓
Mozilla Firefox	✓	✓	×
OpenSSL	✓	✓	×

Tabela 7.3: Resultados obtidos no procedimento de renovação do certificado da AC-Raiz

7.2 Substituição do par de chaves

7.2.1 Sem chave privada disponível

Quando a chave privada da Autoridade Certificadora fica indisponível por algum motivo, é necessária a criação de um novo par de chaves para que esta AC possa continuar operacional, conforme o que foi definido na seção 5.2.1. Para simular esta ação em um ambiente real, o seguinte procedimento foi definido:

a) a estrutura inicial da ICP é criada;

b) o caminho de certificação é verificado;

c) a nova AC-Raiz é criada, com um novo par de chaves e um novo certificado;

d) para cada AC cujo certificado foi emitido pela AC Antiga, são geradas requisições de certificados e enviadas à nova AC;

e) são emitidos certificados para todas as requisições;

f) os novos certificados são adicionados à lista de possíveis certificados do caminho certificação;

g) o caminho de certificação é novamente verificado;

h) remove-se os certificados antigos (AC Raiz antiga e ACs subordinadas antigas);

i) o caminho de certificação é novamente verificado.

Para tornar possível uma análise mais detalhada, foram novamente criados quatro cenários de testes: (I) onde os certificados da AC Raiz nova e das ACs intermediárias apresentam exatamente os mesmos atributos e valores dos certificados antigos, com exceção das datas de validade, valores relacionados às chaves; (II) onde o valor do campo Sujeito do certificado novo da AC Raiz foi modificado; (III) onde o número serial dos certificados das ACs intermediárias foram modificados; e (IV) onde tanto o campo sujeito da AC Raiz nova quanto o número serial dos certificados das ACs intermediárias foram modificados. Para cada um destes cenários foram utilizados os critérios definidos no inicio deste capítulo.

É importante destacar, que neste método de substituição, a principal mudança no ponto de vista de construção do caminho de certificação não se dá na AC Raiz, e sim nas ACs cujos certificados foram emitidos pela AC Raiz. Isto porque a decisão sobre qual caminho de certificação será escolhido e validado é feita exatamente no momento em que os certificados destas AC são encontrados.

7.2.1.1 Resultados

Internet Explorer

Em todos os cenários, a construção do caminho de certificação por nomes foi realizada corretamente, ou seja, a partir do momento em que os novos certificados foram incorporados à lista, o novo certificado da AC de nível 1 foi escolhido automaticamente no caminho de certificação e a partir deste certificado, chegou-se ao certificado da nova AC Raiz. Com o uso do AKID básico a construção do caminho de certificação também foi realizada corretamente em todos os cenários, com comportamento semelhante à construção por nomes.

Já com o uso do AKID completo, os diferentes cenários geraram diferentes comportamentos:

Cenário I – a partir do momento em que os novos certificados foram adicionados, o caminho automaticamente já passou a apontar para os novos certificados;

Cenário II – no momento em que os novos certificados foram adicionados, o caminho continuou apontando para os certificados antigos, pelo fato do valor do campo Sujeito da AC Raiz nova ser diferente da AC Raiz antiga e o conteúdo do campo *authorityCertIssuer* do AKID do certificado de nível 2 do caminho de certificação conter valores que apontam para o campo Sujeito da AC antiga;

Cenário III – quando os novos certificados foram adicionados, o caminho continuou apontando para os certificados antigos, pelo fato do valor número serial do novo certificado da AC de nível 1 ser diferente do valor indicado no campo *authoritySerialNumber* do AKID do certificado de nível 2 do caminho de certificação;

Cenário IV – o caminho continuou apontando para os certificados antigos, pelo fato do valor número serial do novo certificado da AC de nível 1 ser diferente do valor indicado no campo *authoritySerialNumber* do AKID do certificado de nível 2 do caminho de certificação e o campo Sujeito indicado também ser diferente na AC Raiz nova.

Novamente, os resultados dos cenários II, III e IV mostram que os valores das extensões *authoritySerialNumber* e *authorityCertIssuer* foram utilizados corretamente para prover preferência para os certificados.

Com a realização do passo h do procedimento, o caminho foi construído automaticamente até o novo certificado em todos os cenários, mostrando total aderência ao definido nas normas.

Portanto, novamente pode-se afirmar que os testes realizados utilizando o Internet Explorer, além de demonstrarem a eficácia do método, mostram que a implementação da construção do caminho de certificação nesta ferramenta é bastante fiel às normas.

Mozilla Firefox

O navegador Mozilla Firefox possui uma restrição quanto à importação de certificados em sua lista, não permitindo que existam dois certificados que possuam o mesmo número serial e sujeito. Dessa forma, não foi possível comparar a validação do caminho de certificação com a existência dos certificados antigos e novos simultaneamente quando estes possuem o mesmo serial e sujeito (cenários I, II e III).

Devido a esta restrição, os testes realizados nos cenários I, II e III tiveram que sofrer uma alteração no procedimento definido no início desta seção. O passo h teve que ser realizado antes da adição dos novos certificados na lista.

Nos cenários I, II e III a construção do caminho de certificação por nomes e por AKID básico foram realizadas corretamente a partir do momento em que os novos certificados foram adicionados na lista. Embora não tenha sido possível a realização do teste com os certificados antigos presentes na lista, pode-se dizer, baseado nos resultados apresentados no cenário IV, que o caminho construído apontaria para os novos certificados. No caso do AKID completo, o caminho de certificação não foi validado nos cenários II e III, novamente devido ao fato da implementação da montagem do caminho de certificação utilizada pelo Mozilla Firefox não aderir completamente às normas. Já no cenário I, todos os campos eram iguais aos apresentados na extensão AKID, e devido a isso, foi montado corretamente.

No cenário IV, a construção do caminho de certificação por nomes e por AKID básico foram realizadas corretamente a partir do momento em que os novos certificados foram adicionados na lista, apontando automaticamente para os novos certificados. Quando os certificados testados utilizavam a AKID completo, o caminho selecionado foi o que levava aos certificados antigos, onde os campos serial e sujeito eram o mesmos contidos na extensão AKID. Porém, após a remoção dos certificados da lista, o caminho de certificação não foi validado, ou seja, o Firefox não construiu o caminho até a nova AC Raiz.

OpenSSL

Apesar das limitações de construção de caminho de certificação do OpenSSL, os resultados foram os seguintes:

Cenário I – O caminho de certificação foi validado corretamente na construção por no-

mes, por AKID básico e AKID completo, pois todas as comparações realizadas nos valores do Sujeito e das extensões AKID e SKID tiveram resultado positivo;

Cenário II – Na construção por nomes e por AKID básico, o caminho foi montado corretamente até os novos certificados, já que novamente todas as comparações tiveram resultado positivo. Porém no uso do AKID completo, o caminho não foi montado corretamente pelo fato valor apresentado em *authorityCertIssuer* do AKID dos certificados de nível 2 não serem iguais ao valor do Sujeito do certificado da nova AC Raiz;

Cenário III – Novamente na construção por nomes e por AKID básico, o caminho foi montado corretamente, já que novamente todas as comparações tiveram resultado positivo. No uso do AKID completo, o caminho não foi montado corretamente pelo fato valor apresentado em *authoritySerialNumber* do AKID dos certificados de nível 2 não serem iguais ao valor do número serial do certificado da AC Intermediária;

Cenário IV – A construção por nomes e por AKID básico foi realizada corretamente. Com o AKID completo, pelos mesmos motivos apresentados nos cenários II e III, o caminho não foi montado corretamente.

7.2.1.2 Comparação dos resultados

As tabelas 7.4, 7.5, 7.6 e 7.7 mostram as sínteses dos resultados observados nos testes.

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	✓	✓	✓
Mozilla Firefox	✓	✓	✓
OpenSSL	✓	✓	✓

Tabela 7.4: Resultados obtidos no procedimento de substituição do par de chaves da AC Raiz, sem a disponibilidade da chave antiga, no cenário I

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	✓	✓	✓
Mozilla Firefox	✓	✓	×
OpenSSL	✓	✓	×

Tabela 7.5: Resultados obtidos no procedimento de substituição do par de chaves da AC Raiz, sem a disponibilidade da chave antiga, no cenário II

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	✓	✓	✓
Mozilla Firefox	✓	✓	×
OpenSSL	✓	✓	×

Tabela 7.6: Resultados obtidos no procedimento de substituição do par de chaves da AC Raiz, sem a disponibilidade da chave antiga, no cenário III

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	✓	✓	✓
Mozilla Firefox	✓	✓	×
OpenSSL	✓	✓	×

Tabela 7.7: Resultados obtidos no procedimento de substituição do par de chaves da AC Raiz, sem a disponibilidade da chave antiga, no cenário IV

7.2.2 Com chave privada disponível

Conforme descrito na seção 5.2.2, quando se tem a chave privada disponível e deseja-se realizar a troca da chave privada, existem dois casos que podem ser diferenciados. Um onde quando existe a disponibilidade da chave privada de maneira irrestrita e outra onde existem restrições.

7.2.2.1 Com restrições sobre a chave

De acordo com o que foi proposto na seção 5.2.2.1, o operador deverá analisar quais são estas restrições sobre a chave, e consequentemente classificá-las como críticas ou não críticas.

Caso as restrições sejam não críticas, os métodos CMP ou CTL serão utilizados, e por serem métodos já existentes e aceitos atualmente, não foi necessária a realização de testes com eles. Para o CMP, a construção do caminho de certificação é realizada da mesma forma de que é feita no caso de certificação cruzada, com a diferença apenas que todos os novos certificados a serem emitidos pela AC Raiz, serão emitidos através da nova AC Raiz. Para a CTL, a construção do caminho de certificação é de maneira semelhante às Listas Estendidas de Confiança, descrita na Seção 3.5.5. Além do CMP e CTL, pode também ser utilizado o novo método apresentado na Seção 5.2.1. Os resultados dos testes e simulações aplicados sobre este método são os mesmos discutidos e apresentados na seção 7.2.1

Se as restrições forem definidas como críticas, a chave privada antiga não poderá ser utilizada, e devido a isto, o método definido em 7.2.1 deve ser utilizado. Os resultados dos testes e simulações aplicados sobre este método são os mesmos discutidos e apresentados na seção 7.2.1.

7.2.2.2 Sem restrições sobre a chave

Conforme proposto na seção 5.2.2.2, o método a ser utilizado pode ser tanto o CMP quanto o CTL. Para o CMP, a construção do caminho de certificação é realizada da mesma forma de que é feita no caso de certificação cruzada, e para a CTL, a construção do caminho de certificação é de maneira semelhante às Listas Estendidas de Confiança, descrita na Seção 3.5.5. Além do CMP ou CTL, também pode ser utilizado o novo método apresentado na Seção 5.2.1.

7.3 Topologias Dinâmicas

7.3.1 União de ICPs

Quando duas ou mais ICPs desejam se unir e constituir uma hierarquia, o método de União de ICPs definido na seção 6.1 pode ser utilizado. Para simular esta ação em um ambiente real, o seguinte procedimento foi definido:

a) as estruturas iniciais de duas ICPs são criadas;

b) o caminho de certificação é verificado;

c) a nova AC Raiz é criada, com um novo par de chaves e um novo certificado;

d) para cada AC Raiz das ICPs iniciais, são geradas requisições de certificados e enviadas à nova AC Raiz;

e) são emitidos certificados para todas as requisições;

f) os novos certificados são adicionados à lista de possíveis certificados do caminho certificação;

g) o caminho de certificação é novamente verificado;

h) remove-se os certificados antigos de cada ICP;

i) os caminhos de certificação são novamente verificados.

7.3.1.1 Resultados

Internet Explorer

A construção do caminho de certificação por nomes foi realizada corretamente a partir do momento em que os novos certificados foram incorporados à lista. De maneira automática, todos os caminhos de certificação que antes apontavam para as antigas ACs, a partir da adição dos novos certificados na lista, passaram a apontar para o novo certificado de AC Raiz, passando pelos certificados de ACs intermediárias criados. Com o uso do AKID básico a construção do caminho de certificação também foi realizada corretamente, com comportamento semelhante à construção por nomes.

Quando o AKID completo foi utilizado, no momento em que os novos certificados foram adicionados, o caminho continuou apontando para os certificados antigos, pelo fato do valor do campo *authorityCertIssuer* do AKID dos certificados emitidos por cada AC Raiz antiga conter valores que apontam para o campo Emissor do certificado antigo. Com a realização do passo h do procedimento, o caminho foi construído automaticamente até o novo certificado de AC Raiz, mostrando aderência ao definido nas normas.

Portanto, novamente pode-se afirmar que os testes realizados utilizando o Internet Explorer, além de demonstrarem a eficácia do método, mostram que a implementação da construção do caminho de certificação nesta ferramenta é bastante fiel as normas.

Mozilla Firefox

A construção do caminho de certificação por nomes e por AKID básico foram realizadas corretamente a partir do momento em que os novos certificados foram adicionados na lista. Semelhantemente ao comportamento apresentado pelo Internet Explorer, todos os caminhos de certificação que antes apontavam para as antigas ACs, a partir da adição dos novos certificados na lista, passaram automaticamente a apontar para o novo certificado de AC Raiz, passando pelos certificados de ACs intermediárias criados.

No caso do AKID completo, o caminho selecionado foi o que levava aos certificados antigos, onde os campos serial e sujeito eram o mesmos contidos na extensão AKID. Porém, após a remoção dos certificados da lista, o caminho de certificação não foi validado, ou seja, o Firefox não construiu o caminho até a nova AC Raiz, mostrando novamente a não aderência as normas.

OpenSSL

Na construção por nomes e por AKID básico, o caminho foi montado corretamente passando pelos novos certificados e chegando até a nova AC Raiz. Porém no uso do AKID completo, o caminho não foi montado corretamente pelo fato valor apresentado em *authorityCertIssuer* do AKID dos certificados emitidos por cada antiga AC Raiz não serem iguais ao valor do Emissor dos novos certificados.

7.3.1.2 Comparação dos resultados

A tabela 7.8 mostra a síntese dos resultados observados nos testes.

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	✓	✓	✓
Mozilla Firefox	✓	✓	×
OpenSSL	✓	✓	×

Tabela 7.8: Resultados obtidos no procedimento de União de ICPs

7.3.2 Subordinação de ICPs

Quando uma ICP ou mais ICPs desejam se subordinar a uma outra ICP, o método de Subordinação de ICPs definido na seção 6.2 pode ser utilizado. Para simular esta ação em um ambiente real, o seguinte procedimento foi definido:

a) as estruturas iniciais de duas ICPs são criadas;

b) o caminho de certificação é verificado;

c) uma requisição contendo os dados do certificado da AC requisitante é criada;

d) a requisição é enviada para a AC da ICP de destino;

e) a AC de destino emite o certificado;

f) o novo certificado é adicionado à lista de possíveis certificados do caminho certificação;

g) o caminho de certificação é novamente verificado;

h) remove-se o certificado antigo da AC requisitante;

i) os caminhos de certificação são novamente verificados.

7.3.2.1 Resultados

Internet Explorer

A construção do caminho de certificação por nomes foi realizada corretamente a partir do momento em que os novos certificados foram incorporados à lista. De maneira automática, todos os caminhos de certificação que antes apontavam para a antiga ICP, a partir da adição dos novos certificados na lista, passaram a apontar para a AC da ICP de destino, passando pelo novo certificado de AC Intermediária criado. Com o uso do AKID básico a construção do caminho de certificação também foi realizada corretamente, com comportamento semelhante a construção por nomes.

Quando o AKID completo foi utilizado, no momento em que os novos certificados foram adicionados, o caminho continuou apontando para os certificados antigos, pelo fato do valor do campo *authorityCertIssuer* do AKID dos certificados emitidos

pela AC da antiga ICP conter valores que apontam para o campo Emissor do certificado antigo. Com a realização do passo h do procedimento, o caminho foi construído automaticamente até o certificado da nova topologia, mostrando aderência ao definido nas normas.

Mozilla Firefox

A construção do caminho de certificação por nomes e por AKID básico foram realizadas corretamente a partir do momento em que os novos certificados foram adicionados na lista. Semelhantemente ao comportamento apresentado pelo Internet Explorer, todos os caminhos de certificação que antes apontavam para a antiga ICP, a partir da adição dos novos certificados na lista, passaram automaticamente a apontar para a ICP de destino, passando pelo novo certificado de AC intermediária criado.

No caso do AKID completo, o caminho selecionado foi o que levava a ICP Antiga, onde os campos serial e sujeito eram o mesmos contidos na extensão AKID. Após a remoção dos certificados da lista, o Firefox não construiu o caminho até a nova AC Raiz, e consequentemente o caminho de certificação não foi validado, mostrando novamente a não aderência as normas.

OpenSSL

Na construção por nomes e por AKID básico, o caminho foi montado corretamente passando pelos novos certificados e chegando até a nova AC Raiz. Porém no uso do AKID completo, o caminho não foi montado corretamente pelo fato valor apresentado em *authorityCertIssuer* do AKID dos certificados emitidos pela antiga AC não serem iguais ao valor do Emissor dos novos certificados.

7.3.2.2 Comparação dos resultados

A tabela 7.9 mostra a síntese dos resultados observados nos testes.

7.3.3 Emancipação de ACs

Quando uma AC deseja se separar de sua ICP, o método de Emancipação de ACs definido na seção 6.3 pode ser utilizado. Para simular esta ação em um ambiente real, o seguinte procedimento foi definido:

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	✓	✓	✓
Mozilla Firefox	✓	✓	×
OpenSSL	✓	✓	×

Tabela 7.9: Resultados obtidos no procedimento de Subordinação de ICPs

a) a estrutura inicial de uma ICP é criada;

b) o caminho de certificação é verificado;

c) uma requisição contendo os dados do certificado da AC a ser removida é criada;

d) utilizando seu próprio par de chaves, a AC a ser removida emite um certificado auto-assinado;

e) a AC revoga o certificado da AC Removida;

f) o novo certificado é adicionado à lista de possíveis certificados do caminho certificação;

g) o caminho de certificação é novamente verificado;

h) remove-se o certificado antigo da AC Removida;

i) os caminhos de certificação são novamente verificados.

7.3.3.1 Resultados

Internet Explorer

A construção do caminho de certificação por nomes foi realizada corretamente a partir do momento em que o novo certificado foi incorporado à lista. Automáticamente, todos os caminhos de certificação que antes apontavam para a antiga ICP, a partir da adição do novo certificado na lista, passaram a apontar para a nova AC Raiz, que anteriormente se tratava de uma AC Intermediária. Com o uso do AKID básico a construção do caminho de certificação também foi realizada corretamente, com comportamento semelhante à construção por nomes.

Quando o AKID completo foi utilizado, no momento em que o novo certificado foi adicionado, o caminho continuou apontando para os certificados antigos, pelo fato do valor do campo *authorityCertIssuer* do AKID dos certificados emitidos pela antiga AC Intermediária conter valores que apontam para o campo Emissor do certificado antigo. Com a realização do passo h do procedimento, o caminho foi construído automaticamente até o novo certificado de AC Raiz, mostrando aderência ao definido nas normas.

Mozilla Firefox

A construção do caminho de certificação por nomes e por AKID básico foram realizadas corretamente a partir do momento em que o novo certificado foi adicionado na lista. Semelhantemente ao comportamento apresentado pelo Internet Explorer, todos os caminhos de certificação que antes apontavam para a antiga AC Raiz, a partir da adição do novo certificado na lista, passaram automaticamente a apontar para a nova AC Raiz.

No caso do AKID completo, o caminho selecionado foi o que levava a AC Raiz Antiga, onde os campos serial e sujeito eram o mesmos contidos na extensão AKID. De maneira semelhante aos resultados dos testes anteriores, após a remoção dos certificados da lista, o caminho de certificação não foi validado, mostrando a não aderência as normas.

OpenSSL

Na construção por nomes e por AKID básico, o caminho foi montado corretamente até a nova AC Raiz. No uso do AKID completo, o caminho não foi montado corretamente, novamente pelo fato do valor apresentado em *authorityCertIssuer* do AKID dos certificados emitidos pela antiga AC Intermediária não serem iguais ao valor do Emissor do novo certificado.

7.3.3.2 Comparação dos resultados

A tabela 7.10 mostra a síntese dos resultados observados nos testes.

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	✓	✓	✓
Mozilla Firefox	✓	✓	×
OpenSSL	✓	✓	×

Tabela 7.10: Resultados obtidos no procedimento de Remoção de ICPs

7.3.4 Migração de ACs

Quando uma AC deseja remover migrar de uma ICP para outra, o método de Migração de ACs definido na seção 6.4 pode ser utilizado. Para simular esta ação em um ambiente real, o seguinte procedimento foi definido:

a) as estruturas iniciais de duas ICPs são criadas;

b) o caminho de certificação é verificado;

c) uma requisição contendo os dados do certificado da AC a ser removida é criada;

d) a AC revoga o certificado da AC Removida;

e) a requisição é enviada para a AC da ICP de destino;

f) a AC de destino emite o certificado;

g) o novo certificado é adicionado à lista de possíveis certificados do caminho certificação;

h) o caminho de certificação é novamente verificado;

i) remove-se da lista o certificado antigo da AC Removida;

j) os caminhos de certificação são novamente verificados.

7.3.4.1 Resultados

Internet Explorer

A construção do caminho de certificação por nomes foi realizada corretamente a partir do momento em que os novos certificados foram incorporados a lista. De

maneira automática, todos os caminhos de certificação que antes apontavam para a antiga ICP, a partir da adição dos novos certificados na lista, passaram a apontar para a AC da ICP de destino, passando pelo novo certificado de AC Intermediária criado. Com o uso do AKID básico a construção do caminho de certificação também foi realizada corretamente, com comportamento semelhante a construção por nomes.

Quando o AKID completo foi utilizado, no momento em que os novos certificados foram adicionados, o caminho continuou apontando para os certificados antigos, pelo fato do valor do campo *authorityCertIssuer* do AKID dos certificados emitidos pela AC da antiga ICP conter valores que apontam para o campo Emissor do certificado antigo. Com a realização do passo i do procedimento, o caminho foi construído automaticamente até o certificado da nova topologia, mostrando aderência ao definido nas normas.

Mozilla Firefox

A construção do caminho de certificação por nomes e por AKID básico foram realizadas corretamente a partir do momento em que os novos certificados foram adicionados na lista. Semelhantemente ao comportamento apresentado pelo Internet Explorer, todos os caminhos de certificação que antes apontavam para a antiga ICP, a partir da adição dos novos certificados na lista, passaram automaticamente a apontar para a ICP de destino, passando pelo novo certificado de AC intermediária criado.

No caso do AKID completo, o caminho selecionado foi o que levava a ICP Antiga, onde os campos serial e sujeito eram o mesmos contidos na extensão AKID. Novamente, após a remoção dos certificados da lista, o caminho de certificação não foi validado.

OpenSSL

Na construção por nomes e por AKID básico, o caminho foi montado corretamente passando pelos novos certificados e chegando até a nova AC Raiz. No uso do AKID completo, o caminho não foi montado corretamente pelas mesmos motivos dos resultados apresentados nos testes anteriores.

7.3.4.2 Comparação dos resultados

A tabela 7.11 mostra a síntese dos resultados observados nos testes.

	Tipos de Construção		
Ferramenta	**Nome**	**AKID básico**	**AKID completo**
Internet Explorer	✓	✓	✓
Mozilla Firefox	✓	✓	×
OpenSSL	✓	✓	×

Tabela 7.11: Resultados obtidos no procedimento de Migração de ICPs

7.4 Conclusão

No decorrer deste capítulo foram apresentadas a implementação e validação dos métodos discutidos nos capítulos 5 e 6. Foi detalhado o procedimento realizado para a verificação dos testes, bem como as ferramentas utilizadas e suas limitações.

Como resultado destes testes, foi verificada com sucesso a aplicabilidade dos métodos em situações reais, e puderam também ser determinadas as limitações impostas pelas implementações das ferramentas atuais nesses casos. Com isso, mecanismos de contingência para ACs já estabelecidas poderão prever quais os melhores procedimentos para cada situação e implementá-los a partir do conhecimento de suas vantagens e suas limitações.

Durante a realização deste trabalho, foi aberto um registro no site da *Mozilla Foundation* notificando a incompatibilidade da construção do caminho de certificação no navegador *Mozilla Firefox* com as normas definidas pelo padrão X.509. Até o presente momento, a solução do problema não foi realizada.

Devido a não aderência às normas por parte das ferramentas Mozilla Firefox e OpenSSL, se a utilização da extensão AKID completa for necessária e a compatibilidade com estas ferramentas for desejada, pode-se, nos casos onde foram encontrados problemas, estender a reemissão dos certificados, mantendo os mesmos atributos, em mais um nível hierárquico na ICP. Porém, esta medida em alguns casos pode ter custos demasiadamente elevados.

Capítulo 8

Considerações Finais e Trabalhos Futuros

O modelo de gerência de chaves definido neste trabalho é mais abrangente do que os modelos encontrados na literatura. Deve-se lembrar que as técnicas apresentadas no decorrer deste trabalho não implicam na necessidade de alteração do padrão X.509 e sim apresentam maneiras de tratar casos que não estão previstos na literatura, e portanto, podem ser de aplicação imediata.

Para contextualizar o problema em termos das técnicas já previstas na literatura, o Capítulo 4 apresenta os mecanismos atuais para a realização destas substituições. O capítulo seguinte propõe uma nova classificação do problema, com base em várias demandas de substituição de chaves e certificados verificadas em casos reais de infra-estrutura de chaves públicas. Com isto, ficou claro que os métodos disponíveis atualmente não possuem a abrangência necessária para suprir todas as necessidades de uma ICP.

O principal objetivo deste trabalho foi a apresentação de mecanismos que possibilitassem o processo de gerência de ICPs a longo prazo. Foi proposto um mecanismo eficiente para realizar os processos de susbstituição de certificados e chaves de ACs que, além de oferecer compatibilidade com os padrões atuais, preenchem as lacunas deixadas pelos métodos discutidos. A classificação das possíveis operações de substuição de certificados e chaves de ACs apresentada neste trabalho propiciou uma análise mais ampla e abrangente das diferentes situações possíveis de ocorrer em um ambiente real.

Para o caso de substituição do certificado, demonstrou-se que a partir

do certificado antigo é possível realizar sua renovação ou alteração de maneira simples, sem que a topologia da ICP seja afetada. Além disso, mostrou-se viável a implantação de um sistema para a automatização deste processo.

No caso da substituição da chave privada, viu-se que a diferenciação do procedimento de substituição a partir da nova classificação proposta faz com que o impacto da realização deste processo seja menor do que em um procedimento genérico, e além disso, torna possível a solução eficiente de situações não previstas pelas normas.

Uma das principais lacunas preenchidas a partir deste trabalho foi a elaboração de uma solução para restabelecimento de uma Autoridade Certificadora cuja chave privada tenha sido comprometida, ou por algum motivo não se tenha mais a intenção de utilizar esta chave. Esta solução permite um rápido restabelecimento através da criação de uma nova Autoridade Certificadora e a reemissão dos certificados existentes em um nível hierárquico abaixo desta AC, com isso, um novo caminho de certificação é estabelecido sem que sejam gerados impactos em outras entidades pertencentes a esta ICP. A tabela 8.1 apresenta um resumo da comparação desta solução com os métodos previstos na literatura.

Item	CMP	CTL	Nova Substituição
Substituição da chave	obrigatória	opcional	obrigatória
Substituição do certificado	obrigatória	obrigatória	obrigatória
Alteração do Sujeito	impossível	possível	possível
Disponibilidade da chave antiga	obrigatória	obrigatória	desnecessária
Artefatos externos	não utiliza	CTL	não utiliza
Implementação	simples	muito simples	simples
Custo	baixo	muito baixo	baixo

Tabela 8.1: Tabela comparativa dos métodos existentes na literatura com o novo método apresentado

A partir dos os resultados obtidos com a nova classificação e os métodos derivados dela, foi possível a elaboração de outros métodos e aplicações além dos previstos inicialmente. Com isso, novas soluções que vão além das operações de substituição de chaves e certificados de uma AC foram vislumbradas. Estas soluções foram apresentadas no capítulo 6 e permitem modificações dinâmicas na topologia de uma ICP, que podem incluir desde alterações em partes específicas como até em uma ou mais ICPs em sua totalidade. Foram criados 4 novos métodos: União de ICPs, Subordinação de

ICPs, Emancipação de ACs e Migração de ACs.

A união de ICPs apresenta uma significativa redução de custos no processo de estabelecimento de relação de confiança entre duas ICPs, isto porque ocorre uma grande redução do número de certificados emitidos para que esta relação se estabeleça. Além disso, mantém a construção do caminho de certificação de maneira determinística, algo que não ocorre nos métodos convencionais para este fim.

A subordinação de ICPs apresenta um meio de integrar dinamicamente uma ICP já estabelecida a uma outra ICP. Este método, além de evitar um número elevado de reemissão de certificados, pode agregar várias vantagens advindas das características das ICPs envolvidas, como a maior aceitação do ponto de confiança e ampliação do número de entidades confiantes.

A emancipação de ACs permite que uma AC e toda a topologia abaixo dela possam remover seu vínculo com uma determinada ICP e desta forma, tornar-se independente. Isto pode agregar algumas vantagens, como uma maior independência e flexibilidade da AC, além de ter sua aplicação em ambientes organizacionais, onde podem ocorrer situações em que um determinado setor pode se desvincular do restante da organização.

A união de parte do processo de emancipação com o mecanismo de subordinação de ICPs, resultou em um outro método, chamado de migração de ACs. Este método permite que uma AC pertencente a uma ICP remova seu vínculo e passe a se subordinar a uma outra ICP. Com isto, pode-se agregar algumas as vantagens apresentadas no método de emancipação com os benefícios advindos da subordinação de ICPs.

A tabela 8.2 apresenta uma comparação entre os novos métodos. Os itens “Par de chaves”, “Substituição do Certificado” e “Alteração do Sujeito”, referem-se apenas aos certificados reemitidos durante o processo. Se algum certificado é emitido para um nova entidade, como no caso da nova AC Raiz na União de ACs, os resultados apresentados na tabela para estes itens não se aplicam a este novo certificado.

A partir da implementação de um protótipo para validação e testes das propostas apresentadas, foi possível provar que, além de funcionais, as técnicas apresentadas são aplicáveis na prática. Os testes realizados comprovaram a eficiência dos métodos e além disso, puderam gerar uma grande fonte de referência sobre o impacto prático relacionado à aplicação de cada método.

Item	União	Subordinação	Emancipação	Migração
Par de chaves	mantém	mantém	mantém	mantém
Substituição do certificado	obrigatória	obrigatória	obrigatória	obrigatória
Alteração do Sujeito	impossível	impossível	impossível	impossível
Artefatos externos	não utiliza	não utiliza	não utiliza	não utiliza
Implementação	muito simples	muito simples	simples	simples
Custo	muito baixo	muito baixo	baixo	baixo

Tabela 8.2: Comparação dos métodos de topologias dinâmicas

A análise dos resultados da aplicação destes métodos a partir da utilização de ferramentas amplamente difundidas, como Internet Explorer, Mozilla Firefox e OpenSSL, resultou na verificação de algumas diferenças significativas sobre suas implementações. Pôde-se notar algumas divergências sobre a aderência de suas implementações às definições encontradas nas normas, e com isto, problemas foram encontrados e os responsáveis pelas ferramentas foram notificados. A partir desta análise, o operador de uma Autoridade Certificadora poderá prever qual será o impacto de suas ações sobre as aplicações atuais.

Por fim, pode-se dizer que este trabalho, apresenta uma grande evolução do ponto de vista do número de opções quando se deseja realizar modificações sobre uma ICP. Se antes eram encontrados na literatura apenas dois métodos, agora pode-se verificar a existência de mais 5 novos métodos. Com isto, a manutenção de uma ICP a longo prazo é facilitada, já que diferentes situações que antes poderiam paralisar ou até inutilizar toda uma ICP, agora podem ser contornadas de diferentes formas.

Para trabalhos futuros, podem ser exploradas as limitações descritas no início deste trabalho. Uma proposta que pode ser relevante, será a definição do impacto dos métodos apresentados sobre as PCs e DPCs das Autoridades Certificadoras. Este impacto pode ser analisado sob a perspectiva da inclusão de alguns destes métodos no escopo de novos documentos, ou até mesmo sob a utilização destes métodos em uma DPC já existente. Outra contruibuição voltada à estes documentos, é a definição de mecanismos para comparação das PCs e DPCs de diferentes ICPs, isto será importante para facilitar a verificação da aderência entre elas antes da realização de operações que estabeleçam sua relação.

Outra contribuição que pode ser relevante é a verificação e análise da aplicação destes métodos em outros modelos de infra-estruturas de chaves públicas e certificados digitais, tais como o SPKI e o PGP.

Referências

[1] HOUSLEY, R. et al. RFC3280 – certificate and certificate revocation list (crl) profile. Abril 2002. Disponível em: <http://www.ietf.org/rfc/rfc3280.txt>.

[2] ADAMS, C. et al. RFC 4210 – internet x.509 public key infrastructure certificate management protocol (cmp). Março 1999. Disponível em: <http://www.ietf.org/rfc/rfc4210.txt>.

[3] BRASIL. *Medida Provisória 2.200-2*. Agosto 2001. Media Provisória que instituíu a ICP-Brasil.

[4] BRASIL. *Resolução Número. 20*. Maio 2003. Determina o desenvolvimento de uma plataforma criptográfica aberta, voltada à operação da AC Raiz.

[5] ICP BRASIL. *ICP Brasil: Infra-estrutura de Chaves Públicas Brasileira*. Junho 2007. Disponível em: <http://www.icpbrasil.gov.br/>.

[6] ITI. *Programa João de Barro*. Junho 2007. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Swlivre/JoaoDeBarro>.

[7] ELLISON, C. et al. RFC 2693 – spki certificate theory. Setembro 1999. Disponível em: <http://www.ietf.org/rfc/rfc2693.txt>.

[8] CALLAS, J. et al. RFC 2440 – openpgp message format. Novembro 1998. Disponível em: <http://www.ietf.org/rfc/rfc2440.txt>.

[9] STINSON, D. R. *Cryptography Theory and Pratice*. 2. ed. [S.l.]: Chapman & Hall CRC, 2002.

[10] STALLINGS, W. *Cryptography and network security: principles and practice*. 2. ed. [S.l.]: Prentice Hall, 1998.

[11] NIST. *FIPS PUB 46 - Data Encryption Strandard*. 1977.

[12] NIST. *FIPS PUB 197 - Advanced Encryption Strandard*. 2001.

[13] DIFFIE, W.; HELLMAN, M. New directions on cryptographic techniques. *Proceedings of the AFIPS National Computer Conference*, 1976.

[14] HOUSLEY, R.; POLK, T. *Planning for PKI*. 1. ed. [S.l.]: Wiley, 2001.

[15] SALOMAA, A. *Public Key Cryptography*. 2. ed. [S.l.]: Springer, 1996.

[16] RSA. *RSA Security*. Janeiro 2006. Disponível em: <http://www.rsasecurity.com>.

[17] SCHNEIER, B. *Applied Cryptography - Protocols Algorithms, and Source Code in C*. 2. ed. [S.l.]: John Wiley & Sons, 1996.

[18] RYAN, P.; SCHNEIDER, S. *Modeling and Analysis of Security Protocols*. [S.l.]: Addison-Wesley, 2001.

[19] RIVEST, R. RFC 1321 – the md5 message-digest algorithm. Abril 1992. Disponível em: <http://www.ietf.org/rfc/rfc1321.txt>.

[20] NIST. *FIPS PUB 180-1 - Secure Hash Standard*. Abril 1995.

[21] KOHNFELDER, L. *Towards a practical public-key cryptosystem*. [S.l.], 1978.

[22] ITU. *Recommendation X.509 – Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*. [S.l.], 1988.

[23] ITU. *Recommendation X.509 (11/93) – Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*. [S.l.], 1993.

[24] ITU. *Recommendation X.509 (1997 E) – Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*. [S.l.], Junho 1997.

[25] CHOKHANI, S. et al. RFC 3647 – certificate policy and certification practices framework. Novembro 2003. Disponível em: <http://www.ietf.org/rfc/rfc3647.txt>.

[26] PERLMAN, R. Overview of pki trust models. *IEEE Network*, v. 13, n. 6, p. 38 – 43, 1999.

[27] LLOYD, S. Understanding certification path construction. *PKI Forum Technical Group*, Setembro 2002.

[28] LLOYD, S. *AKID/SKID Implementation Guideline*. [S.l.], Setembro 2002.

[29] ITU. *OSI networking and system aspects – Abstract SyntaxNotation One (ASN.1)*. [S.l.], Agosto 2005.

[30] FREEMAN, T. Certificate trust lists: What are they? why are they useful? Presentation at the NIST PKI Working Group meeting. November 1998.

[31] KALISKI, B. Pkcs 7: Cryptographic message syntax. Marco 1998. Disponível em: <http://rfc.net/rfc2315.html>.

[32] JEUN, I. et al. A best practice for root ca key update in pki. In: *ACNS*. [S.l.: s.n.], 2004. p. 278–291.

[33] ADAMS, C.; LLOYD, S. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. 2. ed. [S.l.]: Addison Wesley, 2002. 352 p.

[34] NYSTROM, M.; KALISKI, B. Pkcs #10: Certification request syntax specification version 1.7. Novembro 2000. Disponível em: <http://www.ietf.org/rfc/rfc2986.txt>.

[35] MYERS, M. et al. RFC 4211 – certificate request message format. September 2005. Disponível em: <http://www.ietf.org/rfc/rfc2511.txt>.

[36] HSU, Y.-K.; SEYMOUR, S. P. An intranet security framework based on short-lived certificates. *IEEE Internet Computing*, 1998.

[37] SUTIL, J. M. *Migrando a ICP-Brasil para uma Solução Nacional com Código Livre*. [S.l.], 2007.

[38] MOZILLA FOUNDATION. *Network Security Services (NSS)*. Março 2007. Disponível em: <http://www.mozilla.org/projects/security/pki/nss>.

[39] MICROSOFT. *Cryptographic Application Programming Interface (CryptoAPI)*. Março 2007. Disponível em: <http://msdn2.microsoft.com/en-us/library/aa380255.aspx>.

[40] OPENSSL. *OpenSSL Project*. Janeiro 2006. Http://www.openssl.org/.

Apêndice A

Glossário

Algoritmo Assimétrico – algoritmo usado por cifradores que utilizam par de chaves criptográfias assimétricas (pública/privada).

Algoritmo Simétrico – algoritmo usado por cifradores que utilizam uma chave secreta para cifrar.

Assinatura Digital – transformação de uma mensagem por meio da utilização de uma função de resumo criptográfico e da aplição de criptografia assimétrica sobre este com a utilização da chave privada do assinante.

Autenticidade – garante a identidade de quem está enviando a mensagem.

Autoridade Certificadora – entidade que emite certificados e atesta a veracidade da relação entre entidades e suas respectivas chaves.

Autoridade de Registro – entidade que por delegação de uma ou mais Autoridades Certificadoras desempenha o papel de verificação e registro de dados para estas.

Certificado Digital – estrutura de dados assinada digitalmente por uma AC, contendo informações referentes a seu emissor, seu proprietário e chave chave pública entre outras informações.

Chave Privada – chave mantida secreta por seu proprietário.

Chaves Pública – chave que é divulgada pelo seu proprietário para conhecimento público.

Criptografia – disciplina que trata mecanismos para a transformação de dados, de forma a proteger informações.

Infra-Estrutura de Chaves Públicas – um conjunto de arquitetura, organização, técnicas, práticas e procedimentos para oferecer suporte a implantação e a operação de um sistema de certificação baseado em criptografia de Chaves Públicas.

Integridade – garantia de que o conteúdo da mensagem não sofreu alteração.

Lista de Certificados Revogados – lista contendo informações dos certificados digitais revogados por uma Autoridade Certificadora.

Ponto de Atualização – momento no tempo em que um certificado de AC precisa ser atualizado. Este momento ocorre quando a AC não pode emitir mais certificados digitais pelo fato de seu tempo de validade restante ser inferior ao período de validade que ela atribui aos certificados que emite.

Resumo Criptográfico – um conjunto de dados derivados de uma mensagem que são gerados através de função matemática. Se a mensagem sofrer alteraçoes, o resultado da aplicação desta mensagem alterada à função de resumo gera um conjunto de dados diferente do anterior.

X.509 – Recomendação do ITU-T para o formato de certificados digitais e listas de certificados revogados.