Universidade de São Paulo - USP
Instituto de Matemática e Estatística – IME
Departamento de Ciência da Computação - DCC

TÓPICOS EM CIÊNCIA DA COMPUTAÇÃO

Relatório de Estudo

Aluno: Fábio Correa Xavier
fabiocx@ime.usp.br
Orientador: Routo Terada

1. OBJETIVO

O objetivo deste plano de estudo foi aprofundar o conhecimento do aluno em alguns tópicos relacionados ao assunto envolvido em sua dissertação de mestrado, ou seja aprofundar os conhecimentos do aluno em tópicos relacionados ao funcionamento de Infra-estrutura de Chaves Públicas (*Public-Key Infrastructure* – PKI), conhecer a 4ª edição da recomendação X.509 de 2000, que define o certificado de atributo e a base para a construção de uma *Privilege Management Infrastructure* - PMI.

Todo o estudo foi praticamente baseado na recomendação X.509 da ITU-T de 2000 [1] e na RFC 3281 [18], embora outras fontes foram utilizadas para enriquecer o conhecimento. O primeiro tópico de estudo foi sobre o funcionamento de uma infra-estrutura de chaves públicas. Posteriormente foi feito um estudo sobre os certificados de atributos e sua forma de utilização, definidos na referência [1].

Os tópicos estudados acima descritos serão discutidos nas próximas seções deste relatório.

2. INTRODUÇÃO

É de conhecimento geral que pelo uso de um serviço de autenticação é possível provar quem realmente você é. Certificados de identidade ou certificados de chave pública fornecem a melhor solução para integrar esse serviço de autenticação básico à maioria das aplicações desenvolvidas para a Internet que requeiram o uso de assinaturas digitais.

No entanto, novas aplicações, particularmente na área de comércio eletrônico, necessitam de um serviço de autorização para determinar quais são as permissões ou o papel de um usuário, ou seja, quais são as ações que um certo usuário pode fazer. Nesse caso, privilégios para executar tarefas devem ser considerados.

Um exemplo seria quando uma empresa precisa definir quais serão os privilégios de seus funcionários sobre os recursos disponibilizados por ela, como uma pasta ou documentos de acesso restrito. Nesse caso, o serviço de autorização torna-se importante, pois diferentes conjuntos de privilégios sobre recursos serão atribuídos a diferentes categorias de funcionários. No caso de aplicações distribuídas em que recursos da empresa são compartilhados com empresas parceiras, fornecedores ou clientes, o serviço de autorização torna-se essencial.

A autorização não é um problema recente e diversas soluções foram tentadas no passado. No entanto, as soluções tradicionais não atendem de maneira adequada a diversas aplicações para a Internet. As soluções tradicionais não têm uma fácil implementação em ambientes em que a utilização de certificados de identidade ou certificados de chave pública é necessária. Nesses casos, o uso de objetos de dados independentes que contenham os privilégios do usuário é mais indicado. O certificado de atributo, proposto pela recomendação X.509 da ITU-T (*International Telecommunications Union - Telecommunication*) [1], forneceu uma solução apropriada, que pode ser utilizada em conjunto com certificados de identidade.

Embora o uso de certificados de identidade seja uma boa solução, o seu uso em um serviço de autenticação de grande abrangência só é viável com a implementação de uma estrutura eficiente para gerenciar e distribuir todos os certificados no sistema. Atualmente isso é feito por uma entidade conhecida como Infra-estrutura de Chaves Públicas (ICP), que, ao mesmo tempo, suporta criptografia, integridade e não-repudiação. Sem o seu uso, é praticamente inviável o uso de aplicações com assinatura digital em larga escala.[7][2]

De modo análogo, os certificados de atributos sugeridos pela ITU-T são a base para a construção das Infra-estruturas de Gerenciamento de Privilégios (PMI – *Privilege Management Infrastructure*).

Ambas as infra-estruturas aqui tratadas são independentes, porém, devem ser interconectadas por meio de algum campo comum nos certificados gerados. Esse inter-relacionamento é necessário, uma vez que, para se conceder autorização, é necessário que o evento de autenticação já tenha ocorrido.

Embora interconectadas, ambas as estruturas são autônomas e podem ser gerenciadas independentemente. As tarefas de criação e manutenção de identidades podem ser separadas das tarefas de concessão de autorização. Na verdade, toda a infra-estrutura de autenticação deve estar funcionando antes da implantação de uma estrutura de autorização.

Em ambientes empresariais, essa independência das infra-estruturas é um fator positivo. A razão para isso é que a identidade tem um significado global, cujo certificado pode ser emitido por uma Autoridade Certificadora externa à empresa. Por outro lado, um atributo tende a ter um significado local. Assim, a concessão de privilégios depende

muitas vezes de conhecimento de fatos ou informações confidenciais. Nesses casos, é razoável pensar que a própria empresa, dona das informações, deverá emitir os certificados de atributos necessários.

3. INFRAESTRUTURA DE CHAVES PÚBLICAS (ICP)

Os sistemas eletrônicos de informação atuais são tão complexos quanto as relações de negócios que eles servem. As palavras “Segurança da Informação” são comuns e conhecidas em todos os níveis hierárquicos de uma empresa. A segurança da informação, quando vista de uma perspectiva corporativa, é um facilitador dos objetivos de negócios tradicionais no ambiente eletrônico. Aumentando o faturamento por meio do acesso a novos mercados, reduzindo custos com o uso eficiente de estruturas de *extranet* e Internet para a distribuição de informações, reduzindo o risco de endividamento, tudo isso de forma compatível com as leis governamentais e da indústria, são somente alguns exemplos do quão importante deve ser a política de segurança em uma infra-estrutura de rede. A questão fundamental hoje não é mais se a empresa deve ter uma infra-estrutura de segurança, mas qual infra-estrutura se deve adotar.[14]

Um dos pontos mais cruciais em qualquer transação é a identidade da entidade com a qual a transação está sendo feita. Em uma transação tradicional são utilizados métodos como assinatura de contratos, documentos registrados em cartório ou advogados para ajudar a estabelecer confiança entre as partes em uma relação de negócios. Assim como há vários métodos que garantem a autenticidade das partes em uma transação tradicional, deve haver, em uma transação eletrônica, um método que

garanta a confiabilidade e a autenticidade das partes. De modo similar, a necessidade de confidencialidade na integridade da informação trocada é crítica. Podemos ainda aumentar a lista de serviços de segurança: há a necessidade de estabelecer acordos de não repudiação e, digitalmente, aprovar e, seguramente, datar uma transação. [13]

Como o mundo do comércio está se tornando altamente dependente do armazenamento eletrônico, a acessibilidade a esses dados e a entrega de informação valiosa à manutenção de um bom nível de confiança em todo o processo se torna críticas. Todos os serviços de segurança mencionados anteriormente devem ser utilizados para maximizar as vantagens do comércio eletrônico. A infra-estrutura de chaves públicas (ICP) foi concebida para fornecer uma solução eficiente para a disponibilização dos serviços de segurança, especialmente a autenticação.

A criptografia assimétrica é baseada em um par de chaves. Quando utilizamos um par de chaves, somente uma das chaves, aquela conhecida com chave particular, deve ser mantida em segredo e, geralmente, sob o controle de seu proprietário. A outra chave, conhecida como chave pública, pode ser disseminada livremente para uso por outra pessoa que deseje participar de serviços seguros com a pessoa que possui a chave particular correspondente. Isso é possível porque as chaves são matematicamente relacionadas, mas é computacionalmente difícil gerar a chave particular a partir da chave pública. Em teoria, qualquer individuo pode enviar para o proprietário de uma chave particular uma mensagem criptografada com sua chave pública e somente o proprietário poderá ler a mensagem segura, ou seja, decriptografá-la. De modo análogo, o proprietário de uma chave particular pode estabelecer a integridade e a origem de uma informação enviada para a outra parte se ele assinar digitalmente a informação usando sua chave particular. Qualquer pessoa que receba a informação pode usar a chave pública associada para validá-la, garantindo que a informação veio do proprietário da chave particular, além de se certificar de que a integridade do dado foi mantida.

3.1 A arquitetura de um ICP

Uma Infra-estrutura de Chaves Públicas pode ser definida com um conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revocar certificados de chave pública.

A arquitetura de uma ICP tem se mantido basicamente a mesma desde sua primeira publicação no original *Internet Certificate and Certificate Revocation List* (CRL) *Profile* [15]. O último modelo foi publicado na mais recente versão do *Internet and CRL Profiile* [10]. A Figura 3 -1 - Entidades de uma ICP a seguir ilustra a arquitetura tradicional de uma Infra-estrutura de Chaves Públicas.

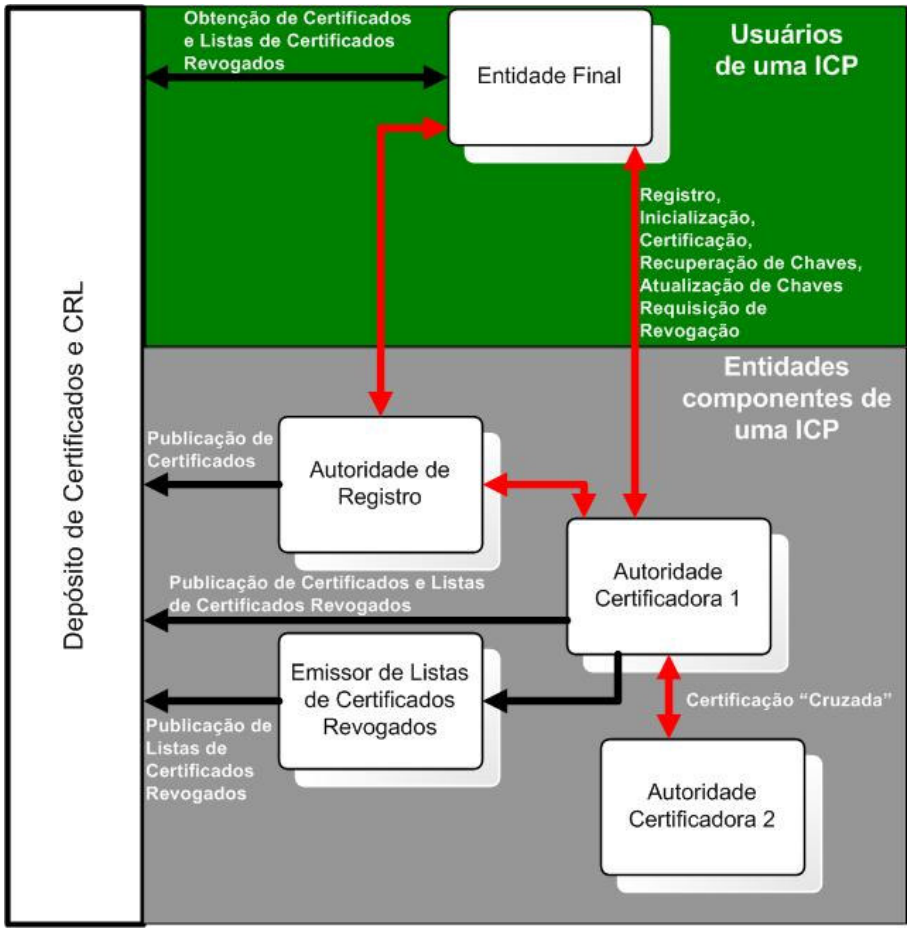

Figura 3 -1 - Entidades de uma ICP

Para melhor entendimento da Figura 3 -1 - Entidades de uma ICP anterior, a Tabela 3-1 - Componentes de um ICP a seguir resume as principais funções das entidades existentes na arquitetura de uma ICP. Tais entidades serão alvo de detalhamento neste capítulo.

Entidade	Principal Função
Entidade Final	Entidade Final é um termo genérico utilizado para designar usuários finais, dispositivos como servidores e roteadores, ou qualquer outra entidade que pode ser identificada no campo sujeito (subject) de um certificado de chave pública. Entidades finais fazem uso ou dão suporte a serviços relacionados a uma ICP.
Autoridade Certificadora (AC)	A Autoridade Certificadora (AC) é o emissor de certificados e Listas de Certificados Revogados (LCR). Ela também pode dar suporte a várias tarefas administrativas, embora tais tarefas sejam geralmente delegadas para uma ou mais Autoridades de Registro.
Autoridade de Registro (AR)	A Autoridade de Registro (AR) é um componente opcional na arquitetura de uma ICP que pode assumir algumas funções administrativas da AC. A AR é freqüentemente associada com o processo de registro da Entidade Final, mas pode também ser útil em várias outras áreas.
Depósito	Um depósito é um termo genérico usado para denotar qualquer método de armazenamento de certificados e Listas de Certificados Revogados de modo que eles possam ser obtidos pelas Entidades Finais.
Emissor de Listas de Certificados Revogados	O Emissor de Listas de Certificados Revogados também é um componente opcional para o qual uma Autoridade Certificadora pode delegar a função de publicação de Certificados.

Tabela 3-1 - Componentes de um ICP

3.1.1 Entidades Finais

Entidades Finais são algumas vezes associadas a usuários finais. Apesar de esse ser freqüentemente o caso, o termo Entidade Final é mais abrangente. Uma Entidade Final pode ser um usuário final como também um roteador, um servidor, um processo ou qualquer coisa que possa ser identificada no campo sujeito (“subject”) de um certificado de chave pública. Outra forma de conceituar o termo Entidade Final é como

sendo um cliente de serviços fornecidos por uma Infra-estrutura de Chaves Públicas. Há casos em que um fornecedor de serviços de ICP pode ser considerado uma Entidade Final. Essa situação existe no relacionamento entre uma Autoridade de Registro e uma Autoridade Certificadora, pois, nesse caso, a Autoridade de Registro está fazendo uso de serviços fornecidos pela Autoridade Certificadora.

3.1.2 Autoridade Certificadora

Chaves públicas são distribuídas na forma de certificados de chave pública. A Autoridade Certificadora (AC) é a principal fundação de uma Infra-estrutura de Chaves Públicas (ICP), uma vez que é o único componente a emitir os certificados de chave pública. Certificados de chave pública são assinados pela Autoridade Certificadora emissora, que amarra o nome do sujeito à chave pública no certificado. Além disso, as Autoridades Certificadoras são responsáveis também pela emissão de Listas de Certificados Revogados (LCR). Esta última função pode ser delegada a uma outra entidade, conhecida como Emissor de Listas de Certificados Revogados.

Autoridades Certificadoras podem também realizar algumas tarefas administrativas, como registro de usuários finais, ou servir como facilitador de recuperação e cópia de segurança de chaves. Porém, nas implementações mais comuns, essas tarefas são delegadas a componentes separados.

3.1.3 Autoridade de Registro

Uma Autoridade de Registro é um componente opcional na arquitetura de uma Infra-Estrutura de Chaves Públicas. Porém, o seu uso pode retirar muitas das tarefas administrativas que uma Autoridade Certificadora assumiria no caso da ausência da Autoridade de Registro. Dentre as atividades executadas por uma Autoridade de Registro temos:

- Verificação de identidade da entidade final que solicitasse o registro em uma ICP;
- Validação dos atributos de sujeito que está solicitando o certificado;

- Verificação se o sujeito realmente possui a chave particular, tarefa conhecida como “prova de possessão”;
- Geração de segredos compartilhados para dar suporte aos processos de certificação e inicialização;
- Geração do par de chaves pública e particular;
- Validação de parâmetros de chaves públicas apresentadas para registro.

É importante ressaltar que, embora a Autoridade de Registro execute muitas funções, ela nunca poderá emitir um certificado de chave pública. Essa tarefa é feita exclusivamente pela Autoridade Certificadora.

O uso inteligente de Autoridades de Registro oferece duas vantagens principais. A primeira é que esse componente ajuda a reduzir os custos envolvidos na criação e manutenção de uma Infra-estrutura de Chaves públicas. Isso é especialmente verdade em empresas grandes e geograficamente dispersas que exigem que seus usuários estejam fisicamente presentes antes que certas atividades relacionadas com uma ICP sejam permitidas. Um exemplo típico é o registro do usuário final, mas outras atividades administrativas de uma ICP, como revogação de certificados ou recuperação de chaves também poderiam se adaptar a essa política. Uma outra situação seria quando a empresa decide terceirizar os serviços de uma Autoridade Certificadora, mas deseja ainda manter o controle sobre o processo de registro.

A segunda grande vantagem é que, aliviando a carga de tarefas administrativas das Autoridades Certificadoras, a empresa pode operar sua AC em modo off-line. Assim, as janelas de oportunidade para ataques remotos são minimizadas.

3.1.4 Depósitos

O termo depósito é freqüentemente associado com um diretório, todavia esse não é necessariamente o caso. Em uma arquitetura de um ICP, um depósito é um termo genérico usado para denotar qualquer método para armazenamento e recuperação de informações associadas a uma Infra-estrutura de Chaves Públicas, como certificados de chave pública e Listas de Certificados Revocados. Um depósito pode ser implementado como um diretório baseado no padrão X.500 com o acesso do cliente por meio de

Ligthweight Directory Access Protocolo (LDAP). O depósito pode ser implementado também de um modo mais simples como, por exemplo, pelo armazenamento das informações em arquivos texto em um servidor remoto cujo acesso pelo cliente pode ser via File Transfer Protocolo (FTP) ou Hyper Text Transfer Protocol (http). Ou seja, o conceito é amplo e abrangente, bem como as implementações possíveis. O grupo de trabalho do Internet Engineering Task Force Public Key Infrastructure (IETF PKI), responsável pela padronização desta estrutura, definiu diversos protocolos operacionais para facilitar a distribuição de certificados de chaves públicas e Listas de Certificados Revogados, incluindo LDAP, HTTP e FTP.

Também é possível retirar a carga de certas funções dos sistemas clientes para uma entidade confiável. Por exemplo, o Online Certificate Status Protocol [16] pode ser usado para perguntar a uma entidade confiável sobre a situação de um ou mais certificados, ou seja, saber se um determinado certificado foi revogado.

O ponto chave aqui é que a entidade final tenha algum mecanismo para consultar os certificados e as listas de certificados revogados. Os depósitos fornecem esse mecanismo para as entidades finais.

3.1.5 Emissor de Listas de Certificados Revogados

O Emissor de Listas de Certificados Revogados, como o próprio nome diz, emite as Listas de Certificados Revogados. A responsabilidade pela emissão de certificados e também pela emissão de Listas de Certificados Revogados é tipicamente de uma Autoridade Certificadora. Entretanto, é possível que a Autoridade Certificadora delegue esta última função para outra entidade. Listas de Certificados Revogados emitidos por outra entidade são chamadas de Listas Indiretas de Certificados Revogados.

3.2 Funções de Gerenciamento de um ICP

Uma Infra-estrutura de Chaves Públicas necessita de algumas funções que "potencialmente precisam ser suportadas por protocolos de gerenciamento" [10]. A **Figura 3 -1 - Entidades de uma** ICP apresenta a interação entre os vários componentes de uma ICP, além de apresentar resumidamente as relações que devem ocorrer entre esses componentes. É importante notar que algumas das funções administrativas podem ser feitas de modo off-line. As seções seguintes abordarão detalhadamente cada uma das funções administrativas referenciadas na Figura 3 -1 - Entidades de uma ICP. Além dessas funções, existem outras opcionais, que serão abordadas mais adiante no capítulo, bem como os protocolos de gerenciamento que devem ser usados para sua realização.

3.2.1 Registro

Entidades Finais devem se matricular em uma Infra-estrutura de Chaves Públicas antes que elas possam utilizar os serviços disponibilizados por uma ICP. O Registro é o primeiro passo no processo de matrícula, que é caracterizado pelo fato de a Entidade Final se apresentar, tornar-se conhecida para uma Autoridade Certificadora [10]. O Registro é usualmente associado com o processo de verificação da identidade de uma Entidade Final. Essa verificação de identidade terá um rigor maior ou menor de acordo com a finalidade do uso do certificado, com políticas associadas ao ICP ou empresa contratante, além do ambiente envolvido. O Registro poderia ser feito diretamente em uma Autoridade Certificadora ou, conforme visto anteriormente, por meio de uma Autoridade de Registro. Esse processo poderia ainda ser totalmente on-line, totalmente off-line ou um misto dos dois anteriores, dependendo das políticas adotadas.

Uma vez que a identidade da Entidade Final é verificada e está de acordo com as políticas adotadas, o componente que está acompanhando o processo de matrícula emite um ou mais segredos compartilhados, além de uma informação de identificação que será utilizada para autenticação quando o processo de matrícula continuar. A distribuição dos segredos compartilhados, por razões de segurança, é feita out-of-band e poderia utilizar segredos compartilhados pré-existentes.

3.2.2 Inicialização

O próximo passo no processo de matrícula é a Inicialização, uma etapa que envolve definir o componente de confiança que atenderá à Entidade Final solicitante. Informações adicionais como aquelas necessárias para atender às políticas para emissão de certificados também devem ser fornecidas pela Entidade Final nessa fase.

A fase de Inicialização é geralmente a criação do par de chaves associado à Entidade Final, isto é, a criação das chaves pública e particular que garantirão a identidade da Entidade Final.

O par de chaves pode ser gerado em vários lugares: a geração pode ser feita por um sistema da Entidade Final, pela Autoridade de Registro, pela Autoridade Certificadora ou um outro componente como um módulo de segurança em hardware. As políticas adotadas pela Infra-estrutura de Chaves Públicas serão as responsáveis por definir onde e por quem o par de chaves poderá ser gerado. Geralmente a limitação se dá pelo ambiente no qual as chaves serão utilizadas.

3.2.3 Certificação

A Certificação é a conclusão do processo de matricula de uma Entidade Final. É nessa fase que será emitido o Certificado de Chave Pública para a Entidade Final. Conforme mencionado anteriormente, a emissão do Certificado de Chave Pública é feita somente pela Autoridade Certificadora. Se o par de chaves foi gerado fora da Autoridade Certificadora, a chave pública que fará parte do Certificado deverá ser passada à AC de uma maneira segura.

Após a emissão, o Certificado de Chave Pública é enviado à Entidade Final e pode ser publicado no Depósito, possibilitando consultas.

Embora as fases de registro, inicialização e certificação sejam independentes, elas podem ser agrupadas em um único protocolo de operação [10].

3.2.4 Recuperação do Par de Chaves

O par de chaves pública e particular é usado para a criação e verificação de assinaturas digitais, criptografia e decriptografia de mensagens ou ambas as situações.

Quando uma chave pública é utilizada para criptografar uma mensagem, em alguns casos é importante termos um mecanismo de recuperação da chave particular quando o acesso a esta não é mais possível, por alguma razão válida. Caso a recuperação da chave não seja possível, a recuperação da mensagem original também não será. A chave particular pode se tornar indisponível por inúmeras razões, como esquecimento de senhas, discos rígidos danificados, estrago ou perda de token, dentre outros. A função administrativa de recuperação de par de chaves permite que uma entidade final obtenha novamente seu par de chaves de uma entidade autorizada, tipicamente uma Autoridade Certificadora.

Existem outras situações nas quais a recuperação de chaves é válida, como aquelas em que a relação da Entidade Final com sua Empresa muda, no caso de uma demissão, por exemplo, e a empresa necessita recuperar informações que foram criptografadas com o par de chaves daquela Entidade Final. Há ainda a possibilidade de que a informação criptografada seja requerida por alguma medida judicial, independente da vontade da Entidade Final. Para esses casos, a recuperação de chaves torna-se uma função vital, embora a maioria das políticas de segurança proíba tal atitude.

3.2.5 Atualização do Par de Chaves

Os certificados são emitidos com uma validade definida. Embora em alguns casos a validade seja bem generosa, em algum momento o certificado expirará. A atualização do par de chaves pode também ser solicitada quando da revogação de um determinado certificado, função a ser discutida na próxima seção.

A atualização do par de chaves envolve a geração de um novo par de chaves e a conseqüente emissão de um novo certificado de chave pública para a Entidade Final. Essa função é distinta da função de Emissão de novo Certificado, na qual não há a geração de um novo par de chaves, mas apenas a emissão de um novo certificado de chave pública.

O processo de atualização do par de chaves pode ser feito em seguida a uma expiração de certificado, mantendo a Entidade Final sempre de posse de um certificado válido. Esse procedimento não é recomendado pelo PKIX Working Group para uso na Internet [10], embora seja possível estabelecer períodos de validade diferentes para as chaves particulares e públicas, usadas, respectivamente, para assinar e verificar uma

assinatura. Essa situação cria uma janela, na qual uma informação assinada com uma chave particular expirada possa ser validada e verificada por uma chave pública ainda válida, até que o processo de atualização do par de chaves esteja finalizado.

3.2.6 Requisição de Revogação

Como mencionado anteriormente, os Certificados de Chave Pública são geralmente emitidos com um prazo de validade muito grande. Tal situação pode gerar um problema: o Certificado pode não ser mais válido antes que seu prazo de validade expire. Essa situação pode ocorrer quando há o comprometimento da chave particular, quando há uma mudança na relação da Entidade Final com a empresa, quando há mudança de nome, dentre outras.

Para esses casos, existe a possibilidade de se revogar o Certificado emitido antes da expiração do prazo de validade. A Requisição de Revogação permite a uma Entidade Final ou uma Autoridade de Registro revogar um dado Certificado de Chave Pública. Para essa função, podem ser utilizados mecanismos out-of-band, e, em alguns casos, a Entidade Final nem precisa, ou nem deve, ser envolvida no processo.

A informação de que houve um determinado Certificado revogado deve ser publicada e se tornar disponível para os usuários. Essa função é responsabilidade da Autoridade Certificadora que emitiu o Certificado ou pode ser delegada para um Emissor de Listas de Certificados Revogados. A freqüência de publicação é altamente dependente das políticas e do ambiente para o qual o Certificado foi emitido. Esse processo é exibido na **Figura 3 -1 - Entidades de uma** ICP anterior.

É importante ressaltar que as Entidades Finais, ou terceiros operando com essas, devem verificar se os Certificados envolvidos nas transações ainda são válidos. Para isso, não basta verificar a data de validade; é necessário também consultar a lista de certificados revogados.

3.2.7 Certificação Cruzada

O processo de certificação cruzada ocorre entre Autoridades Certificadoras distintas, ou seja, um certificado cruzado é um certificado de chave pública que é emitido por uma Autoridade Certificadora para outra Autoridade Certificadora. Em outras palavras, um certificado cruzado é um certificado de chave pública que contém a chave pública de uma Autoridade Certificadora e é assinado por outra Autoridade Certificadora.

A certificação cruzada pode ser uni ou bidirecional. A certificação unidirecional ocorre tipicamente em um modelo de confiança hierárquico, no qual Autoridades Certificadoras superiores emitem certificados cruzados para Autoridades Certificadoras subordinadas. Nesse modelo, uma Autoridade Certificadora subordinada nunca emite um certificado cruzado para uma Autoridade Certificadora superior.

A certificação cruzada bidirecional ocorre entre Autoridades Certificadoras, podendo uma Autoridade emitir um certificado para a outra e vice-versa.

3.3 Funções de Gerenciamento Adicionais

Nas seções anteriores, foram abordadas as funções típicas de uma Infra-estrutura de Chaves Públicas [10]. Entretanto, existem algumas funções adicionais que podem ser úteis e necessárias em alguns cenários, e o PKIX working group reconhece essas funções e os protocolos definidos para dar suporte a elas. Algumas dessas funções adicionais incluem [17]:

- Divulgação de atualização de chave da Autoridade Certificadora – fornece um mecanismo para que uma Autoridade Certificadora divulgue que seu par de chaves foi trocado.
- Divulgação de Certificado – fornece um método para divulgação de um certificado quando os métodos tradicionais, como o depósito, não estão disponíveis.
- Divulgação de Revogação – fornece um método para informar à Entidade Final que seu Certificado de Chave Pública foi ou será revogado.
- Divulgação de Listas de Certificados Revogados - fornece um método para a Autoridade Certificadora divulgar que uma nova Lista de Certificados Revogados foi emitida.

- Confirmação do Certificado – essa função é usada pela Entidade Final para explicitamente aceitar ou rejeitar o Certificado de Chave Pública que foi emitido para ela.
- Arquivo de Chaves – usado para explicitamente requisitar a recuperação da chave particular, usada na decriptografia de informações criptografadas, descrita na seção 0 - 3.2.4 Recuperação do Par de Chaves.

O Arquivo de Chaves, além de ser utilizado para dar suporte à operação de Recuperação do Par de Chaves, pode também ser utilizado para armazenamento de chaves particulares por um longo período, bem como para armazenamento de certificados de chave públicas usadas para verificação de assinaturas. Essa situação é desejável em diversos cenários. Ela permite que Entidades Finais recuperem as chaves utilizadas durante um período longo, permitindo a criação de um histórico de chaves. O histórico, por sua vez, permite que seja possível a verificação de assinaturas que foram feitas há muito tempo, mesmo com a utilização de chaves que já expiraram. Isso pode ser útil na validação ou revalidação de documentos antigos, assinados com chaves antigas.

3.4 Arquiteturas de uma Infra-estrutura de Chaves Públicas

As Autoridades Certificadoras podem ser interligadas de várias formas. Para atender às necessidades da empresa ou órgão que fará uso de uma ICP, uma arquitetura para implementação da solução deverá ser adotada. Existem duas arquiteturas tradicionais da ICP disponíveis: a arquitetura hierárquica ou a arquitetura mista.

3.4.1 Arquitetura Hierárquica

Na arquitetura hierárquica, as autoridades são dispostas hierarquicamente abaixo da AC raiz. Nesse modelo, ocorre apenas a certificação cruzada unidirecional, ou seja, apenas as Autoridades Certificadoras superiores emitem certificados para as Autoridades subordinadas.

Numa ICP hierárquica, todas as partes confiáveis conhecem a chave pública da AC raiz. Qualquer certificado pode ser validado pela da verificação do caminho de validação dos certificados da AC raiz. Como exemplo, vamos observar a **Figura 3-2 - Arquitetura Hierárquica de uma ICP** a seguir. Se a Entidade Final 1 deseja manter uma comunicação confiável com a Entidade Final 2, o certificado de chave pública dessa precisa ser validado. Após essa validação, a Entidade Final 1 tem que validar o certificado a entidade que emitiu o certificado da Entidade Final 2, neste caso a Autoridade Certificadora 4. Após essa validação, o processo deve continuar até que seja atingida a Autoridade Certificadora Raiz, cuja chave pública é conhecida de todos, inclusive da Entidade Final 1, que iniciou esse processo, conhecido como caminho de certificação.

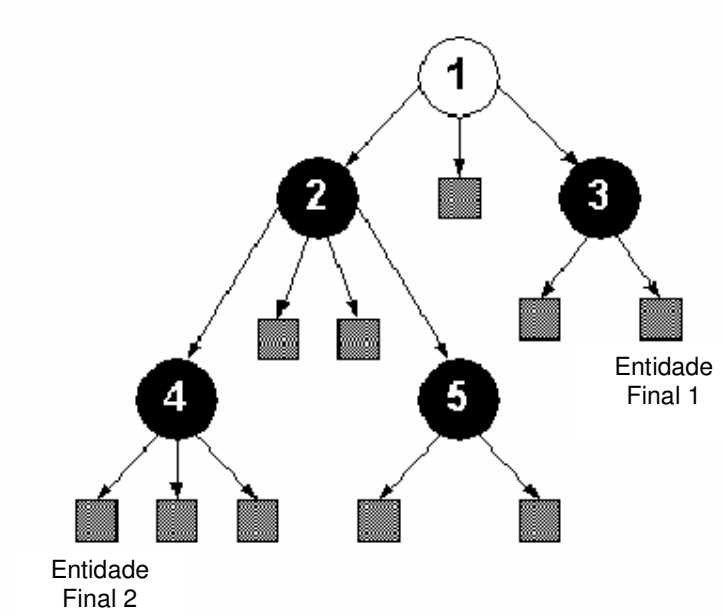

Figura 3-2 - Arquitetura Hierárquica de uma ICP

3.4.2 Arquitetura Mista

Na arquitetura mista, existem várias Autoridades Certificadoras independentes que se autenticam mutuamente, ou seja, nesse caso há a autenticação cruzada bidirecional. O resultado dessas autenticações cruzadas é a criação de inúmeras relações de confiança entre as ACs parceiras. Uma parte confiável conhece a chave pública de uma AC próxima a ela mesma, geralmente a mesma que emitiu seu certificado. A parte

confiável valida o certificado pela verificação do caminho de validação dos certificados que derivam daquela AC parceira. Como exemplo, vamos observar a **Figura 3-3 - Arquitetura Mista de uma ICP** a seguir. A Entidade Final 1 conhece a chave pública da AC 3, e a Entidade Final 2, por sua vez, conhece a chave pública da AC 4. Existem vários caminhos de certificação que conduzem a Entidade Final 2 até Entidade Final 1. O mais curto requer que a Entidade Final 1 valide o certificado da Entidade Final 2, emitido pela AC 4, aí o certificado da AC 4 emitido pela AC 5 e, finalmente, o certificado da AC 5 emitido pela AC 3. A AC 3 é a AC da Entidade Final 1, que confia nela e conhece sua chave pública.

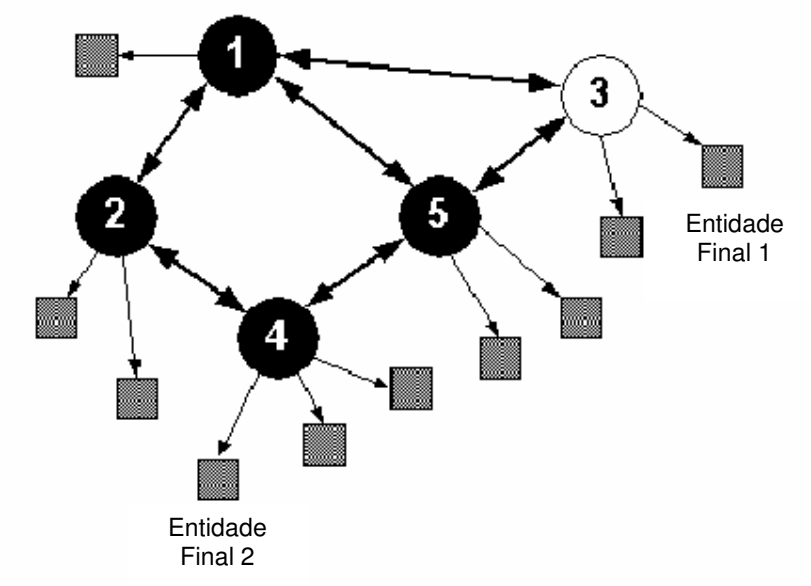

Figura 3-3 - Arquitetura Mista de uma ICP

3.5 Certificados de chave pública X.509

Desde a sua primeira versão, os certificados de chave pública X.509 criados pela IETF evoluíram muito em busca de uma maior flexibilidade, estando atualmente em sua terceira versão. O certificado de chave pública X.509 pode ser utilizado para transportar vários tipos de informações, que são colocadas em dois tipos de campos pré-definidos: os obrigatórios e os opcionais.

Para permitir que o certificado seja válido, ele é assinado digitalmente pelo seu emissor. Assim, os usuários dos certificados têm apenas que verificar a assinatura do

emissor para validarem o certificado. Uma vez validado, as informações de um certificado de chave pública X.509 são confiáveis.

Os certificados possuem um conjunto padrão de campos e podem incluir um número opcional de extensões. Existem dez campos padrão: seis obrigatórios e quatro opcionais. A **Figura 3-4 - Certificado X.509** a seguir exibe estes campos.

Os campos obrigatórios são:

1. número de série;
2. algoritmo identificador da assinatura do certificado;
3. nome do emissor do certificado;
4. período de validade do certificado;
5. chave pública; e
6. nome do sujeito.

O sujeito é a Entidade Final que detém o controle da chave particular correspondente à chave pública do Certificado. Os quatro campos opcionais são:

1. número da versão;
2. dois identificadores únicos, sendo um do Emissor e o outro do Sujeito; e
3. extensões.

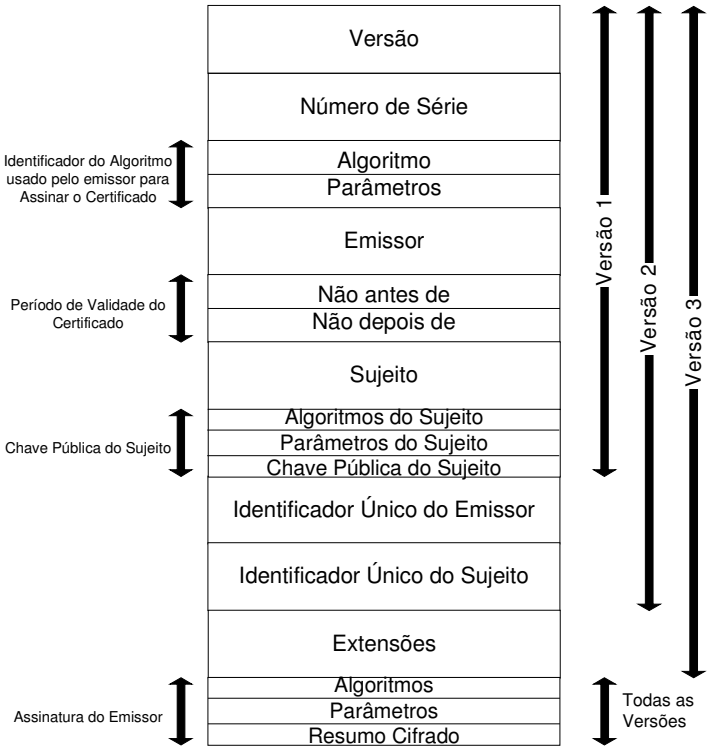

Figura 3-4 - Certificado X.509

Os campos opcionais aparecem somente nos certificados das versões 2 e 3. O campo versão descreve justamente que versão do certificado está sendo utilizada. Como esse campo é opcional, quando ele não existir, o certificado será tratado como na sintaxe da versão original, ou seja, da versão 1.

As diferenças fundamentais entre as versões dos certificados estão na quantidade de campos tratados. Os certificados da versão 1 não possuem identificadores únicos para o emissor e o sujeito, nem extensões. Os certificados da versão 2 já incluem identificadores únicos, mas sem extensões. Quando o certificado inclui extensões, como acontece com a maioria deles atualmente, o campo versão indica versão 3.

O número serial é um número inteiro atribuído pelo emissor para o certificado. O número serial deve ser único para cada certificado gerado pelo emissor. Essa condição é exigida porque torna possível a identificação unívoca de qualquer certificado, pela combinação do nome do emissor e do número serial.

O campo assinatura indica o algoritmo utilizado pelo emissor para assinar o certificado emitido.

O campo emissor contém o nome único padrão X.500 da autoridade confiável que emitiu o certificado.

O campo validade indica o período de validade do certificado, descrevendo a data inicial e final deste período.

O campo sujeito contém o nome único da Entidade Final que detém a chave particular correspondente à chave pública contida no certificado.

O campo Chave Pública do Sujeito contém informações sobre a chave pública do sujeito: além da própria chave pública, esse campo contém o nome do algoritmo usado para gerar as chaves e alguns parâmetros adicionais que foram utilizados na geração do par de chaves.

Os campos de identificadores únicos para o emissor e para o sujeito contêm os números de identificação dessas entidades e só aparecem nos certificados da versão 2 ou 3. Os identificadores únicos do sujeito e do emissor são utilizados para permitir a reutilização dos nomes do sujeito ou do emissor. Entretanto, essa reutilização não é recomendada quando se exige um alto grau de segurança. Portanto, a utilização desses campos também não é recomendada nesses casos.

O campo Extensões, que só existe nos certificados da versão 3, podem ser utilizados para acrescentar mais informações ao certificado. As extensões mais comuns de certificados foram definidas pelo ISO para a ANSI, para resolver questões que não podiam ser resolvidas pelos campos originais.

Essas extensões possibilitam que uma Autoridade Certificadora inclua informações que normalmente não seriam fornecidas pelos campos originais de um certificado. Qualquer empresa pode definir suas extensões próprias, de acordo com suas necessidades.

As extensões possuem três componentes: identificador, um sinalizador de criticidade e um valor. O identificador mostra o formato e a semântica do campo valor. O sinalizador de criticidade indica a importância da extensão. Quando esse sinalizador estiver ligado, significa que essa informação é essencial para o uso do certificado. Portanto, se um sinalizador de criticidade desconhecido for encontrado, o certificado poderá não ser aceito ou, no melhor caso, ser ignorado.

3.6 Principais vulnerabilidades da Infra-estrutura de Chaves Públicas

O processo de emissão de certificados de chaves públicas envolve, além da emissão propriamente dita, algumas tarefas criticas que colocam algum risco no processo. Tarefas como garantir a identidade dos assinantes; determinar o conteúdo apropriado para o certificado digital; criar, distribuir, garantir a aceitação do Certificado, além de promover a segurança interna devem ser tratadas com o máximo de cuidado pela Autoridade Certificadora. As seções seguintes abrangem algumas tarefas que expõe a Autoridade Certificadora à riscos de segurança e integridade.

3.6.1 Verificação de Identidade

O primeiro passo para o registro de uma Entidade Final é a verificação da identidade desta Entidade. Para confirmar a identidade de uma Entidade Final, a Autoridade Certificadora verifica as credenciais fornecidas pela Entidade. Esta função também pode estar delegada para uma Autoridade de Registro, que deverá verificar a identidade da Entidade Final.

O risco no processo de verificação de Identidade está no fato de haver uma falsa confirmação de identidade, ou seja, a AC ou a AR validam a identidade de uma Entidade Final falsa. A conseqüência seria a perda de confiança na estrutura que foi criada para ser uma entidade de confiança. Além disso, a AC estará sujeita a sanções judiciais cabíveis.

O cuidado com a identidade não se restringe ao processo de verificação. Pode ser que a identidade anteriormente verificada sofra alguma mudança de situação e, de acordo com as políticas adotadas, a partir desta mudança, ela não atenda mais aos requisitos. Assim, faz-se necessária uma auditoria constante nas identidades das Entidades finais para as quais foram emitidos Certificados de Chave Pública.

3.6.2 Validade do certificado

Os campos que compõem o certificado variam de versão para versão. O campo mais importante de um certificado, especialmente quanto à segurança, é o campo de validade. Quanto mais distante for a data de expiração de um certificado, maior será o risco assumido pela Autoridade Certificadora que o emitiu. A segurança de um certificado passa por vulnerabilidades físicas e lógicas que extrapolam o software utilizado para gerar a assinatura digital. Quanto mais tempo esse software estiver em uso, maiores são as chances dele ser corrompido ou de que alguém consiga um acesso não autorizado.

3.6.3 Criação, distribuição e aceitação dos certificados

O processo de criação, distribuição e documentação do histórico de aceitação do certificado de um determinado assinante expõem a AC aos riscos relacionados à transação, à estratégia e à reputação. Na criação do certificado, os riscos de transação e de reputação aparecem a partir de possíveis erros nos sistemas que atribuem as limitações apropriadas para cada certificado dependendo das características únicas de cada assinante. A exposição a esses riscos está associada às políticas e procedimentos que regem esse processo. A distribuição e aceitação dos certificados, muitas vezes não é uma tarefa exclusiva das ACs. O cliente terá que obter recursos tecnológicos para criar assinaturas digitais a partir de um fornecedor de software ou outra empresa de tecnologia.

Entretanto, o certificado não estará completo enquanto a AC não atestar a capacidade de assinatura do cliente com a sua própria assinatura digital antes de gerar o certificado. Em um sistema de AC fechada, o risco pode ser limitado pelo contrato que estabelecerá claramente as tarefas e responsabilidades das partes envolvidas. O risco envolvido em uma transação pode ser creditado a uma organização, ao cliente individual e nas partes envolvidas ou uma outra entidade que tenha a guarda do banco de dados de certificados. Todavia, a AC terá um risco na sua reputação se algum problema com a tecnologia for a ela atribuído. Geralmente, um certificado digital não poderá ser usado até que o assinante aceite o certificado assinado. A aceitação implica que o cliente concorda com os termos e condições estabelecidos pela AC para o sistema como um todo, assim como qualquer outra condição específica que seja aplicada ao assinante. Erros que forem

gerados durante o processo de comunicação relativos a aceitação quer seja por dificuldades técnicas ou por políticas e procedimentos inadequados, expõem a AC a riscos na sua reputação e transação.

3.6.4 Gerenciando Certificados Digitais

Quando a AC emite um certificado para suportar a assinatura digital de um cliente, a AC normalmente irá interagir somente com o cliente ou seu representante, ou um agente agindo em nome dele. Todavia, se a AC optar por também gerenciar certificados de terceiros, por exemplo atuando como um repositório, a AC irá transacionar com as entidades que recebem as mensagens. A discussão a seguir descreve os riscos que irão surgir quando lidamos com o serviço de repositório para o assinante e parceiros. Ela esta organizada de forma a abordar os quatro aspectos do gerenciamento de chaves digitais:

- Revelação de informações sigilosas sobre o cliente;
- Serviços e suporte ao assinante;
- Suspendendo e revogando certificados; e
- Processando os pedidos dos parceiros

3.6.5 Revelação de informações sigilosas sobre o cliente

Apesar de não haver até o momento uma legislação específica acerca de revelação de informação, a AC terá que fornecer alguma informação abrangendo os serviços básicos ofertados e os direitos e responsabilidades dos assinantes e de seus parceiros. A natureza da quebra do sigilo terá impactos no risco à reputação e à transação da AC. Por exemplo, se forem divulgados claramente a política de privacidade e os procedimentos para resolução de erros de uma AC, pode haver menos confusão por parte dos usuários. Além disso, se a AC fornecer documentação técnica sobre o uso do software que for associado aos certificados, os assinantes terão melhores condições para

distinguir problemas causados pelo software ao invés de culpa-la, evitando, dessa forma, riscos na reputação da AC.

3.6.6 Serviços e suporte ao assinante

Como muitos dos novos produtos e serviços da tecnologia de informação, a AC precisa fornecer suporte aos seus clientes, o que é uma fonte para o risco de reputação. A AC deverá possuir um sistema de suporte via telefone ou alguma outra forma de interação direta com os assinantes e seus parceiros. As políticas, procedimentos e operações do atendimento telefônico são uma fonte em potencial de riscos para a reputação e transação. Resolver os problemas ou erros que os assinantes e seus parceiros irão encontrar devido à falta de familiaridade com o uso da tecnologia envolvida irá requerer recursos substanciais por parte da AC ou de uma empresa de serviços contratada. Apesar de a AC normalmente não fornecer software para a criação de assinaturas digitais, podem ocorrer situações em que o assinante atribua a AC toda a sua dificuldade em usar a tecnologia.

Os assinantes podem ter problemas técnicos devido à configuração dos softwares em seus computadores pessoais que podem não estar descobertas antes de eles tentarem assinar uma mensagem ou uma transação. Se uma organização que fornece serviços de AC desejar manter um bom relacionamento com seus clientes, a decisão mais prática pode ser o fornecimento deste serviço com recursos próprios ou através da contratação de uma empresa com experiência no ramo. Algumas empresas de tecnologia fornecem um cartão inteligente (smart card), para armazenar o certificado do assinante. Ao invés de copiar o software para o disco rígido do seu computador pessoal, o assinante manteria um leitor de cartão inteligente conectado ao seu PC. O cartão inteligente e o leitor seriam programados previamente para carregar a informação do certificado do assinante apropriadamente. Podemos reduzir os riscos de reputação e de transação pela simplicidade no uso do hardware mencionado, ao invés de requerer do usuário a utilização de software de fontes externas.

3.6.7 Suspendendo e revogando certificados

Existe a possibilidade de o sistema ser comprometido e ficar disponível para uso não autorizado devido à responsabilidade do assinante na guarda da assinatura. Portanto, a AC pode ser acionada para suspender ou revogar um certificado. Se a AC (ou outra entidade responsável dentro do sistema), não monitorar e tomar as medidas necessárias dentro do tempo necessário, a AC pode autenticar mensagens ou transações que carregam uma assinatura digital expirada. Assim, uma AC que não cancelar rapidamente um certificado inválido, estará potencialmente exposta a riscos em sua reputação, estratégia e transação. As políticas e os procedimentos inadequados são uma fonte para o risco estratégico, e se forem implementadas, expõem a AC aos riscos de reputação e transação. O intervalo de tempo das atualizações necessárias no repositório pode variar de acordo com o tipo de certificado envolvido; um atraso na suspensão de um certificado usado em transações ou mensagens importantes significa um risco alto.

Um certificado digital pode ficar inválido de duas formas. A AC pode cancelar o certificado se ela tiver certeza que o assinante tenha tido a sua capacidade de assinar comprometida. O caso mais comum seria a perda da chave privada por parte do usuário. Se a chave privada do usuário tornar-se conhecida, pessoas não autorizadas poderiam assinar mensagens e transações. Se houver qualquer dúvida sobre o status de um certificado, ele deve ser suspenso até que sua situação possa ser determinada. Os riscos de reputação e de transação podem ser resultados de erros no processamento, na suspensão ou do cancelamento de certificados. Por exemplo, o usuário cujo certificado foi equivocadamente suspenso e está impossibilitado de assinar mensagens, poderá sofrer perdas e pode demandar medidas legais, denegrindo a reputação da AC no processo. Por outro lado, uma AC também pode ficar exposta se um parceiro aceitar uma mensagem ou transação que foi assinada por um usuário cujo certificado deveria ter sido revogado ou suspenso.

3.6.8 Processando as Requisições dos Parceiros

O processamento das requisições dos parceiros relativas ao status de certificados individuais pode expor uma AC aos riscos de reputação, estratégia e de transação. Apesar de a relação contratual entra a AC e o usuário definir algumas obrigações aos assinantes e terceiros, essa proteção contratual pode não existir nas

transações com os parceiros, principalmente em sistemas abertos. Por exemplo, se a AC apresenta um certificado revogado como operacional para um parceiro, a AC estará exposta a perda de reputação ou ao recebimento de demandas judiciais. Existe um risco adicional em sistemas abertos se as circunstâncias de um usuário ou grupo de usuários mudarem durante o período de validade de um certificado que está circulando. Qualquer atraso no processamento das requisições de cancelamento de certificados que forem causadas por falhas de políticas e procedimentos ou falhas operacionais, podem resultar nesse tipo de erro. A exposição ao risco é maior ainda, se o repositório processar as requisições no modo "batch" ao invés de "tempo real". Conforme aumenta o volume de transações processadas pelo repositório, e mais certificados forem colocados em circulação, carregando limitações variadas e datas de expiração, a exposição ao risco também aumenta.

3.6.9 Revogação de certificados

Existem dois métodos reconhecidos para responder a uma requisição sobre a validade de um certificado. O mais conhecido requer que o repositório recupere uma longa lista de certificados inválidos, a Lista de Certificados Revogados (LCR), para verificar a validade de um único certificado. As inconsistências em uma LCR são uma fonte de risco na transação para a AC. Adicionalmente, a freqüência programada para a geração das LCRs irão afetar a exposição a riscos do repositório. A geração mais freqüente de LCRs, irá reduzir a exposição ao risco de transação e de reputação. Também existe uma questão sobre como o status do certificado deve ser conhecido pelos parceiros; ou a AC o envia ("push") ou eles buscam o status no repositório da AC ("pull").

Existem diferentes exposições de risco de reputação e de transação associados a cada método. O método "pull" permite ao repositório da AC transferir com sucesso qualquer risco de reputação para o parceiro, caso ele aceite um certificado inválido.

Por outro lado, o método "push" claramente coloca a responsabilidade na AC, caso a LCR não esteja corrigida ou distribuída no tempo necessário. Devido aos riscos e aos custos dessa abordagem, a indústria está desenvolvendo um segundo método. Algumas empresas de tecnologia desenvolveram um software que permite que um repositório procure em seus próprios registros pela validade de um único certificado em

tempo real. Outra fonte de risco de transação do repositório é aquela relacionada à capacidade do parceiro em entender as extensões dos certificados.

4. AUTORIZAÇÃO COM CERTIFICADOS DE ATRIBUTOS

Os certificados de chave pública X.509 vinculam uma identidade a uma chave pública. Um certificado de atributo (AC) não contém chave pública, Um certificado de atributo contém atributos que especificam privilégios de um grupo, usuário, papel ou outra informação de autorização associada com o proprietário do AC. A sintaxe para o certificado de atributo também é definida na Recomendação X.509 da ITU-T, tornando o termo “certificado X.509” ambíguo.

Há uma confusão comum no mercado acerca dos certificados de chave pública e do certificado de atributos. Como analogia, um certificado de chave pública pode ser considerado como um passaporte: ele identifica o proprietário, tende a ter uma validade longa, e o processo de obtenção não é dos mais triviais. Um certificado de atributos, por sua vez, pode ser comparada a um visto de entrada: ele é geralmente emitido por uma autoridade diferente e seu prazo de validade é curto. Além do mais, para requerer um visto de entrada é necessário apresentar o passaporte e o seu processo de obtenção é, na maioria das vezes, mais simples [2].

Para fornecer informações de autorização com certificados X.509, podem-se utilizar dois métodos: colocar essa informação em uma extensão do certificado de chave pública ou utilizar um certificado de atributos. A primeira opção é geralmente indesejada

por duas razões principais. A primeira é que o tempo de vida da autorização é geralmente menor que o tempo de vida da identidade e da chave pública. Quando essas informações estão em um mesmo certificado, o que ocorre é que o tempo de vida do certificado de chave pública é reduzido para se adequar às exigências da informação de autorização. O segundo motivo é que o emissor do certificado de chave pública não é usualmente o mais indicado para conceder autorização. Essa situação geraria passos adicionais para obter as informações de autorização no processo de emissão do certificado de chave pública.

Por essas razões, a melhor opção geralmente é utilizar um certificado de atributos para separar as informações de autorização do certificado de chave pública. Ao adotar essa solução, deve haver um meio de se vincular uma identidade, atestada pelo certificado de chave pública, aos seus privilégios. O certificado de atributos fornece uma solução para essa situação.

Um certificado de atributos pode ser utilizado também para fornecer serviços de não-repudiação. Nesse contexto, os atributos contidos no certificado fornecem informação adicional sobre a entidade que emitiu o certificado, garantindo a originalidade do certificado.

O uso de certificados de atributos permite que a delegação de privilégios. O padrão X.509 [1] define autorização como sendo “transporte de privilégios de uma entidade que possui algum privilégio para outra entidade” [2]. Os certificados de atributos, que são um método de autorização, são muito eficientes para delegar privilégios de uma entidade para outra, permitindo até mesmo a substituição.

4.1 Formas de distribuição de certificados de atributos

Os certificados de atributos fornecem informações de autorização para uma infinidade de ambientes, incluindo aplicações, acessos físicos, acessos lógicos, dentre outros. Para que o certificado seja utilizado, ele deve ser apresentado ao objeto que fará uso dessas informações de autorização. Para isso, existem dois métodos principais: *push* e *pull*.

Em alguns ambientes, é desejável que o usuário apresente seu certificado de atributos para um servidor. Esse é o método *push*, que isenta o servidor de solicitar ou procurar o certificado de atributos em uma terceira entidade, melhorando o desempenho do sistema como um todo. Além disso, o cliente apresenta ao servidor somente os atributos que o servidor precisa saber. Esse modelo é especialmente útil em arquiteturas intra-domínios, na qual os privilégios de um usuário devem ser atribuídos dentro do domínio do original do usuário.

Em outros casos, é interessante que o usuário somente se autentique no servidor, que deverá solicitar (método *pull*) ao emissor ou a um depósito o certificado de atributos desse usuário. A principal vantagem do modelo *pull* é que não é necessária nenhuma modificação no lado do cliente. Ou seja, a forma de comunicação cliente-servidor permanece inalterada. Entretanto, uma carga de trabalho extra é passada para o servidor. A esse é atribuída a tarefa de solicitar e verificar o certificado de atributo do usuário. Esse modelo é especialmente útil em arquiteturas inter-domínios, na qual os privilégios de um usuário devem ser atribuídos dentro do domínio do servidor ao invés do domínio original do usuário.

4.2 A arquitetura de um PMI

A quarta edição da recomendação ITU-T X.509 de 2000 apresenta quatro modelos de uma *Privilege Management Infrastructure* – PMI: modelo geral, modelo de controle, modelo com delegação e modelo com papéis.

As seções seguintes abordam cada um desses modelos.

4.2.1 Modelo Geral

O modelo de gerenciamento de privilégio geral é composto de três entidades: o objeto, o declarador de privilégio e o verificador de privilégio.

O objeto pode ser um recurso a ser protegido que possui métodos que podem ser solicitados pelo declarador de privilégio. Como exemplo, considerando que o objeto é um diretório em um servidor, os métodos de leitura ou gravação podem ser solicitados.

O declarador de privilégio, por sua vez, é a entidade que detém privilégios que são declarados quando necessário.

O verificador de privilégio é a entidade que determina se os privilégios declarados são suficientes ou não para um dado contexto.

A decisão de autorizar ou não o acesso depende basicamente de quatro aspectos:

- Privilégios apresentados pelo declarador de privilégio;
- Política de privilégios adotada, ou seja, que privilégios são necessários para obter o acesso a um determinado método do objeto;
- Variáveis de ambiente atuais, se for o caso;
- Sensibilidade do método do objeto, se relevante.

A Figura 4-5 – Modelo geral de uma PMI abaixo exibe o modelo geral de uma PMI.

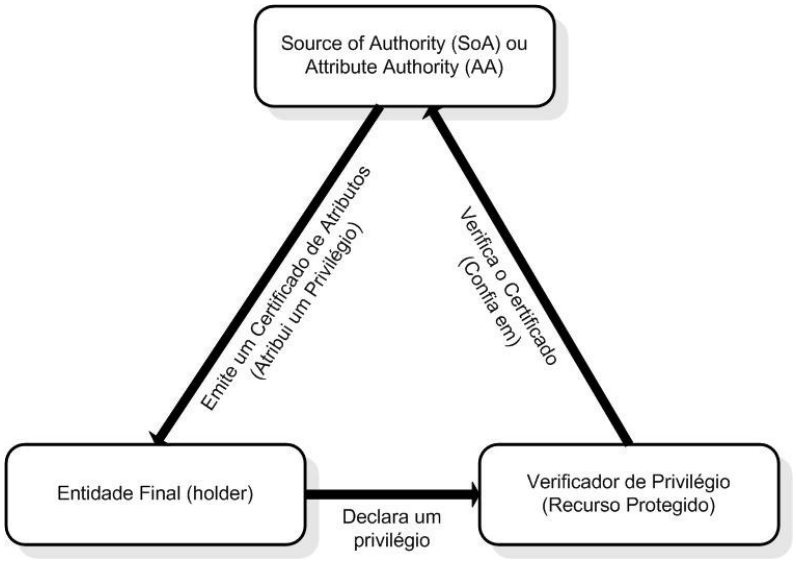

Figura 4-5 – Modelo geral de uma PMI

O privilégio que uma entidade possui reflete o grau de confiança que o emissor do certificado tem nessa entidade, além de manter a aderência às políticas de autorização adotadas.

As políticas de privilégio especificam o grau de privilégio que é suficiente para uma dada sensibilidade do método do objeto ou um dado contexto de uso. As políticas podem ser das mais variadas possíveis, variando de políticas locais a políticas universais, de acordo com a estratégia da empresa. Em outras palavras, a política de privilégio define

um limite mínimo aceitável de um dado conjunto de privilégios [1] que garantirão o acesso ao método desejado. Desta forma, o verificador de privilégios tem como decidir de maneira precisa quando um declarador de privilégio terá ou não o acesso requisitado.

A sensibilidade do método do objeto pode refletir atributos do documento ou requisição, como saldo de uma conta para autorização de transferência ou saldo da cota de impressão de um usuário, ou também o grau de confidencialidade do conteúdo de um documento.

4.2.2 Modelo de Controle

O modelo de controle não é um modelo de arquitetura propriamente dito, mas é um modelo conceitual que ilustra como o certificado de atributo pode ser utilizado para controlar o acesso a um determinado método do objeto. Este modelo consiste de cinco componentes, a saber:

Declarador de privilégio que tem o privilégio e o apresenta ao verificador de privilégio;

- O verificador de privilégio, que decide se os privilégios apresentados são suficientes para garantir o acesso ao método desejado;
- O método do objeto a ser requisitado; que pode ter uma sensibilidade;
- A política de privilégio adotada na empresa ou instituição;
- As variáveis de ambiente que influirão na decisão a ser tomada pelo verificador de privilégio.

A Figura 4-6- Modelo PMI com controle exibe o modelo aqui apresentado.

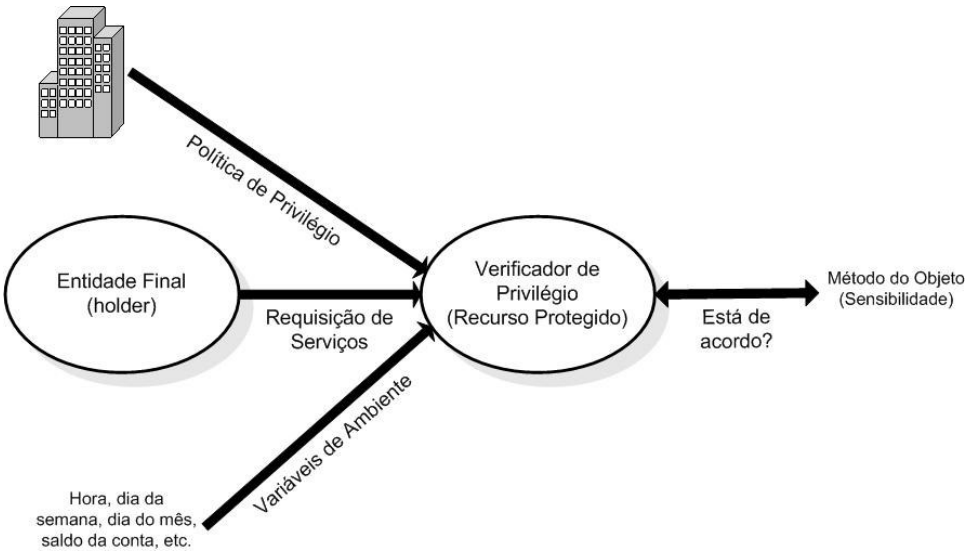

Figura 4-6- Modelo PMI com controle

4.2.3 Modelo com delegação

Em muitos ambientes, existe a necessidade de se delegar alguns privilégios à outras entidades. Pensando nisso, a quarta edição da recomendação X.509 da ITU-T definiu um modelo que possibilita essa delegação. O modelo com delegação é composto basicamente de quatro elementos: o verificador de privilégios, o SOA, outras autoridades de atributo e o declarador de privilégio.

O SOA – *Start of Authority* – é o emissor inicial de certificados que atribuem privilégios a entidades. No modelo geral visto anteriormente, só existe o SOA, que é uma autoridade de atributos que emite os certificados de atributos. No modelo com delegação, o SOA além de atribuir privilégios, também autoriza que a entidade para a qual o certificado foi emitido também atue como uma autoridade de atributo. Assim, o proprietário de privilégios que detém alguns atributos, pode delegar o todo ou parte desses atributos a outras entidades, emitindo para elas um certificado de atributo. Esse proprietário de privilégios, uma autoridade de atributo, também pode autorizar essas outras entidades a delegar os privilégios recebidos.

A Figura 4-7 - Arquitetura PMI com delegação a seguir ilustra o modelo com delegação.

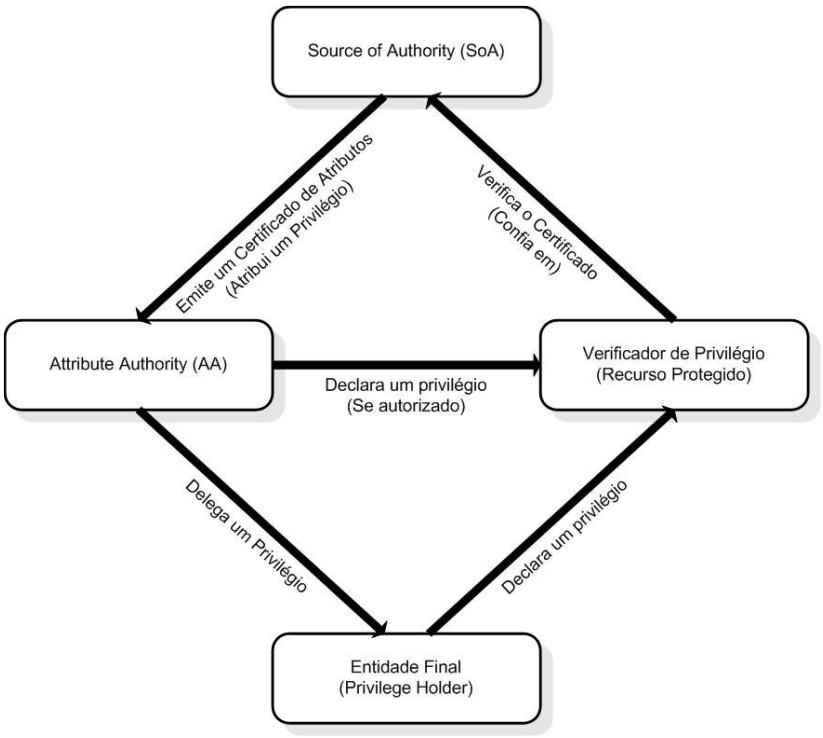

Figura 4-7 - Arquitetura PMI com delegação

A SOA pode impor restrições à cadeia de AA, por exemplo, limitando o comprimento dessa cadeia ou o conjunto de privilégios que podem ser delegados. Uma restrição universal é que nenhuma AA pode delegar mais privilégios do que ela possui.

Quando a delegação é usada, o verificador de privilégios confia na SOA para delegar algum ou todos os privilégios para as entidades. Se o certificado apresentado por um declarador de privilégio não foi emitido pela SOA, o verificador de privilégio deve verificar todo o caminho de delegação, ou seja, verificar todos os certificados emitidos pelas AA intermediárias até alcançar a SOA. Essa validação deve verificar inclusive se cada AA tem os privilégios suficientes para a emissão dos certificados, além de garantir que a AA tem a permissão de delegar privilégios.

Quando se utilizam certificados de atributos para atribuir privilégios, todo o caminho de delegação deve ser feito pela emissão de certificados de atributos. Por outro lado, quando se utilizam certificados de chave pública para atribuir privilégios por meio da extensão *subjectDirectoryAttributes*, todo o caminho de delegação deve ser feito com certificados de chaves públicas.

4.2.4 Modelo de papéis

Papéis fornecem um meio de se atribuir indiretamente privilégios à indivíduos. Para os indivíduos são emitidos certificados de atribuição de papel que atribuem um ou mais papéis a ele. Os privilégios são atribuídos aos papéis através de certificados de especificação de papel, ao invés da atribuição direta a entidades finais por meio de certificados de atributos. Este mecanismo permite que se altere o privilégio de um papel, sem qualquer necessidade de alteração ou operação, como revogação, do certificado de atribuição de papel emitido para as entidades.

A Figura 4-8 - Modelo PMI com suporte a papéis exibe o modelo de uma PMI com papéis.

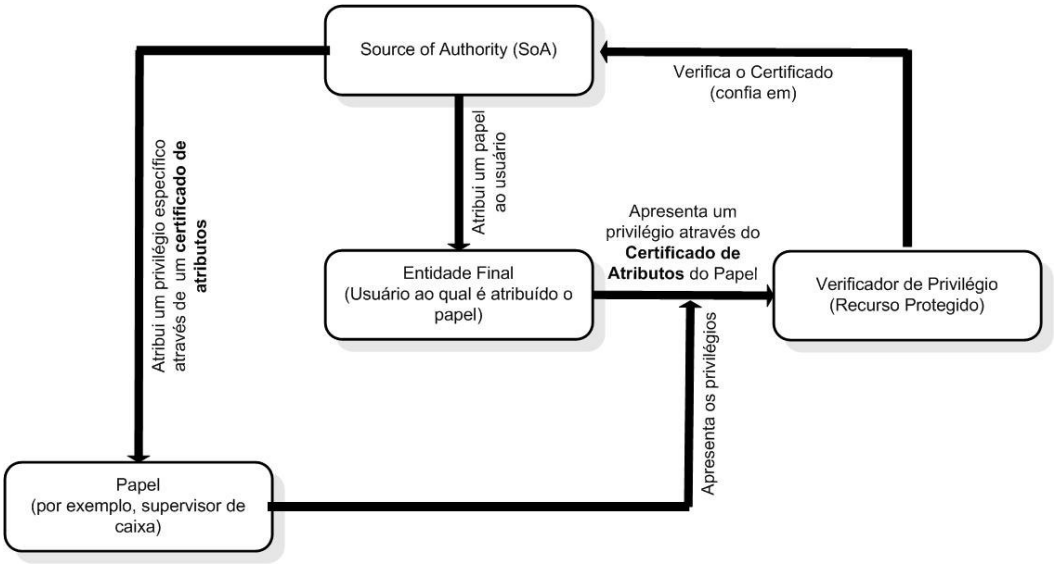

Figura 4-8 - Modelo PMI com suporte a papéis

Os certificados de atribuição de papel podem ser certificados de atributos ou certificados de chave pública. Certificados de especificação de papel só podem ser certificados de atributo[1].

Quadro resumo das entidades de uma PMI

A Tabela 4-2 - Componentes de uma PMI consolida as informações das seções anteriores, exibindo as principais entidades de uma PMI, bem como suas funções, independente do modelo arquitetural adotado.

Entidade	Principal Função
Start of Authority (SOA)	Entidade que emite e assina certificados de atributos, sendo equivalente ao CA raiz de uma PKI.
Autoridade de Atributo (AA)	Entidade que emite e assina o certificado de atributo, em alguns casos chamada de emissora do certificado de atributo.
Usuário do certificado de atributo ou declarador de privilégio	Qualquer entidade que faz uso ou processa um certificado de atributo
Verificador de privilégio	Qualquer entidade que verifica a validade de um certificado de atributo e então faz uso do resultado. Geralmente é a entidade protegida pelo esquema de autorização implementado.
Depósito ou repositório	Um depósito é um termo genérico usado para denotar qualquer método de armazenamento de certificados e Listas de Certificados Revogados de modo que eles possam ser obtidos pelas Entidades componentes do sistema.

Tabela 4-2 - Componentes de uma PMI

4.2 Premissas do modelo

O modelo proposto na referência [18] apresenta algumas premissas que devem ser observadas pelos implementadores. Essas premissas são classificadas em premissas de validade, tipos de atributos, objetivo do certificado e método de apresentação do certificado.

Quanto à validade do certificado de atributo, o modelo permite o uso de um tempo de vida curto tanto quanto um tempo de vida longo. Um período de validade curto, geralmente é definido em horas, enquanto que um período longo é definido em meses. Deve-se, no entanto, observar que o uso de curtos períodos de validade permite que um certificado seja confiável sem o uso de mecanismos de revogação. Essa característica

simplifica o modelo, além de acrescentar uma maior confiabilidade. Por outro lado, períodos de validade longos evitam a necessidade constante da emissão de novos certificados para seus usuários.

Quanto ao tipo de atributo, a autoridade de atributo (AA) deveria ser capaz de definir os tipos de atributos específicos para uso dentro de seus domínios. A AA deve também ser capaz de definir e trabalhar com tipos de atributos padrão, além de poder diferenciar o uso de um mesmo atributo em domínios diferentes. Um exemplo é o grupo de administradores definido no domínio IME e o grupo de administradores definido no domínio POLI. Embora o atributo seja o mesmo – grupo de administradores – o contexto em que eles são válidos são diferentes. Essa diferença deve ser facilmente identificada pela AA.

Quanto ao objetivo de um certificado de atributo, deve-se definir um servidor ou um pequeno grupo deles que serão o alvo para o uso do certificado. Em outras palavras, isto significa que um servidor que não esteja definido como “alvo”, embora confiável, rejeitará as decisões de autorização contidas no certificado.

Finalmente, quanto ao método de apresentação do certificado, o modelo define dois métodos – *push* e *pull* – já apresentados anteriormente. O certificado de atributo deveria ser definido de modo que ambos os métodos sejam suportados. Essa premissa é importante porque torna o modelo flexível o suficiente para atender as necessidades e políticas de qualquer empresa.

4.3 Certificados de atributo X.509

A recomendação X.509 da ITU-T contém a definição de um certificado de atributo apresentada a seguir no padrão *Abstract Syntax Notation One* - ASN.1 [11].

```
AttributeCertificate ::= SEQUENCE {
        acinfo              AttributeCertificateInfo,
        signatureAlgorithm  AlgorithmIdentifier,
        signatureValue      BIT STRING
}
```

***AttributeCertificateInfo* ::= SEQUENCE {**

version	***AttCertVersion*** – a versão é a 2 (v2),
holder	***Holder***,
issuer	***AttCertIssuer***,
signature	***AlgorithmIdentifier***,
serialNumber	***CertificateSerialNumber***,
attrCertValidityPeriod	***AttCertValidityPeriod***,
attributes	**SEQUENCE OF *Attribute***,
issuerUniqueID	***UniqueIdentifier* OPTIONAL**,
extensions	**Extensions OPTIONAL**.

}

***AttCertVersion* ::= INTEGER { v2 (1) }**

***Holder* ::= SEQUENCE {**

baseCertificateID [0] ***IssuerSerial* OPTIONAL**,

- Emissor e número de série do proprietário do Certificado de chave pública.

entityName [1] ***GeneralNames* OPTIONAL**,

- nome do requerente.

objectDigestInfo [2] ***ObjectDigestInfo* OPTIONAL**

- Usado para diretamente autenticar o proprietário do certificado, por exemplo, um arquivo executável.

}

***ObjectDigestInfo* ::= SEQUENCE {**

digestedObjectType **ENUMERATED {**

publicKey (0),
publicKeyCert (1),
otherObjectTypes (2)

}

- otherObjectTypes não deve ser usado segundo o modelo aqui apresentado.

otherObjectTypeID **OBJECT IDENTIFIER OPTIONAL**,
digestAlgorithm *AlgorithmIdentifier*,
objectDigest **BIT STRING**
}

AttCertIssuer **::= CHOICE {**
v1Form ***GeneralNames***,
v2Form **[0]** ***V2Form***

- Esta versão 1 não deve ser usada neste modelo. Usar somente a versão 2.

}

V2Form **::= SEQUENCE {**
issuerName ***GeneralNames*** **OPTIONAL**,
baseCertificateID [0] ***IssuerSerial*** **OPTIONAL**,
objectDigestInfo [1] ***ObjectDigestInfo*** **OPTIONAL**

- o campo issuerName deve estar presente para atender a este modelo, enquanto que baseCertificateID e objectDigestInfo não devem estar presentes.

}

IssuerSerial **::= SEQUENCE {**
issuer ***GeneralNames***,
serial ***CertificateSerialNumber***,
issuerUID ***UniqueIdentifier*** **OPTIONAL**
}

AttCertValidityPeriod **::= SEQUENCE {**
notBeforeTime **GeneralizedTime**,
notAfterTime **GeneralizedTime**
}

Embora a sintaxe de atributo esteja definida em [10], essa é repetida a seguir por conveniência:

Attribute **::= SEQUENCE {**

type ***AttributeType***,

values **SET OF *AttributeValue***

– Ao menos um valor é necessário.

}

AttributeType **::= OBJECT IDENTIFIER**

AttributeValue **::= ANY DEFINED BY *AttributeType***

A opção *GeneralName*, que identifica os participantes no processo, oferece grande flexibilidade. Quando falamos de interoperabilidade, a flexibilidade tem que ser limitada. Assim, o uso da opção *GeneralName* é restringida pelo modelo proposto pela referência [18]. Essas restrições se baseiam na definição de que opções podem ser utilizadas em *GeneralName*. Para que uma implementação esteja de acordo com o modelo proposto, as opções *dNSName, directoryName, uniformResourceIdentifier* e *iPAddress* devem ser suportadas [10].

Além disso, as implementações não devem permitir o uso das opções *x400Address, ediPartyName ou registeredID em GeneralName*.

A figura a seguir mostra o certificado de atributo anteriormente definido.

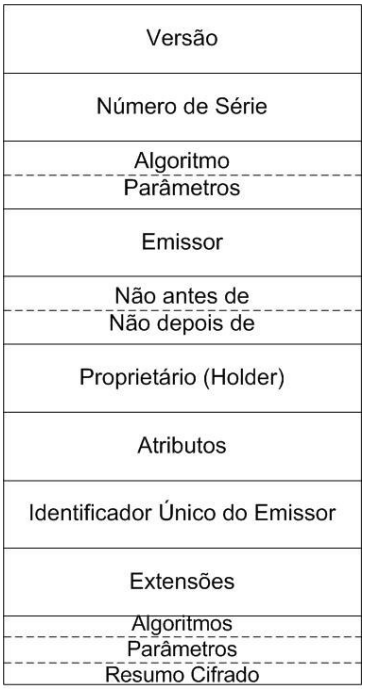

Figura 4-9 - Certificado de Atributo

As seções seguintes apresentam uma descrição da sintaxe dos campos padrão de um certificado de atributo.

4.3.1 Versão

Esse campo deve ser definido como versão 2.

A versão 2 não é compatível com a versão 1 anterior, definida na recomendação X.509 de 1997.

4.3.2 Proprietário (Holder)

Esse campo é um seqüencial que permite três sintaxes diferentes: *baseCertificateID, entityName e objectDigestInfo*. Essas opções podem ser utilizadas em conjunto ou individualmente. Para evitar confusão sobre qual opção é normativa e qual seria uma dica, é recomendável utilizar somente uma das opções acima no campo proprietário do certificado de atributos.

Nos ambientes onde o certificado de autorização é passado em uma mensagem ou sessão autenticada e onde essa autenticação é baseada no certificado de chave pública, o campo proprietário deveria conter a opção *baseCertificateID*. Quando utilizamos essa opção, o campo proprietário do certificado de atributo é idêntico ao campo número serial do certificado de chave pública. Isto é desejável, uma vez que se forma aí o vínculo necessário entre a identidade de um objeto e a autorização fornecida por infra-estruturas diferentes. A figura a seguir mostra o vínculo criado através da opção *baseCertificateID*.

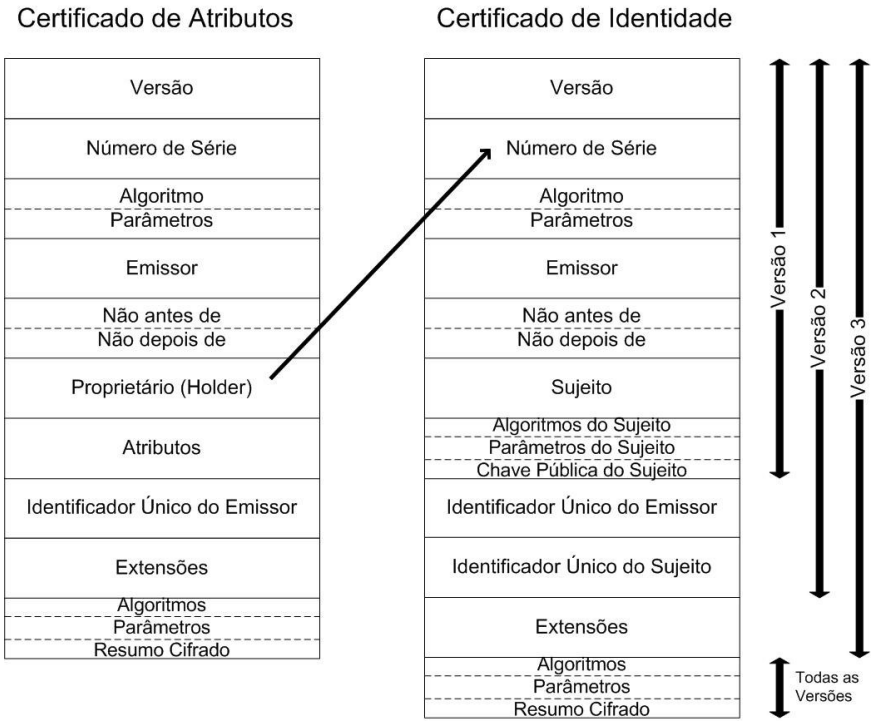

Figura 4-10 - Vínculo através da opção *BaseCertificateID*

Existe a possibilidade de se utilizar a opção *entityName* no campo proprietário. Nesse caso, a *entityName* deve ter o mesmo valor colocado no campo sujeito do certificado de chave pública, caso uma infra-estrutura de chave pública seja a autoridade de autenticação. Assim o vínculo entre a identidade e a autorização está mais uma vez garantido. A figura a seguir mostra o vínculo criado com a opção *entityName*.

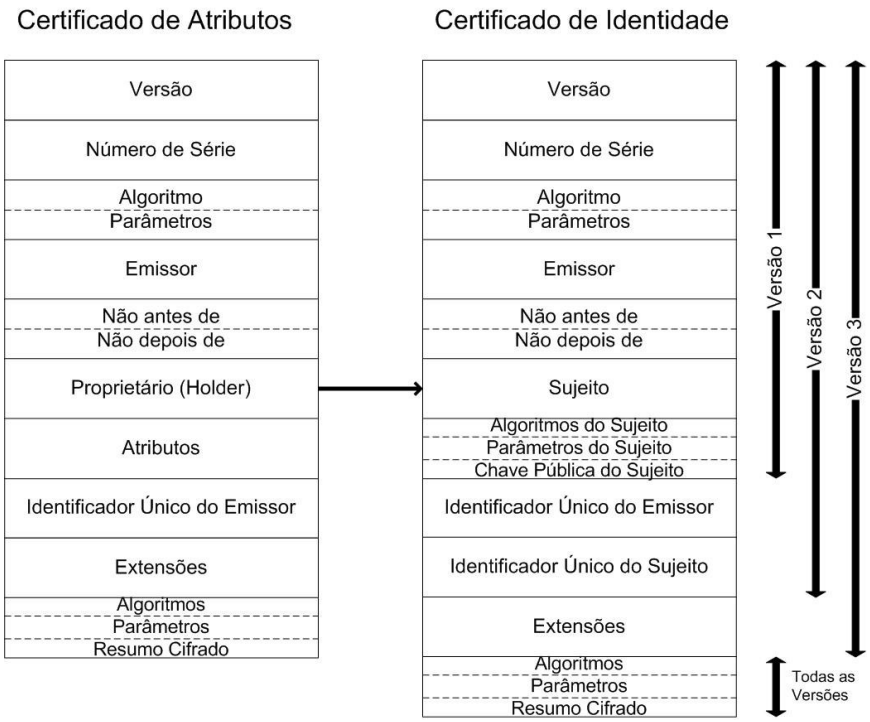

Figura 4-11 - Vínculo através da opção *EntityName*

A última possibilidade para o campo proprietário é a utilização da opção *objectDigest*. Essa opção é utilizada quando não se deseja vincular um certificado de atributo diretamente a uma entidade, através da opção *entityName*, ou a um certificado de chave pública, através da opção *baseCertificateID*.

Uma vez que a opção *objectDigestInfo* é utilizada no campo proprietário, o certificado de atributo deve ser da versão 2, indicada no campo versão desse certificado.

O objetivo da opção *objectDigestInfo* é permitir vincular o certificado de atributo à um objeto, como um programa Java ou até mesmo diretamente à uma chave pública, através de uma função *hash* desse objeto. O resultado dessa função *hash* seria então colocado no campo proprietário do certificado de atributo. O padrão proposto na referência [18] só reconhece o uso da opção *objectDigestInfo* para uso em chaves públicas, desconsiderando qualquer outro objeto, embora seja tecnicamente viável.

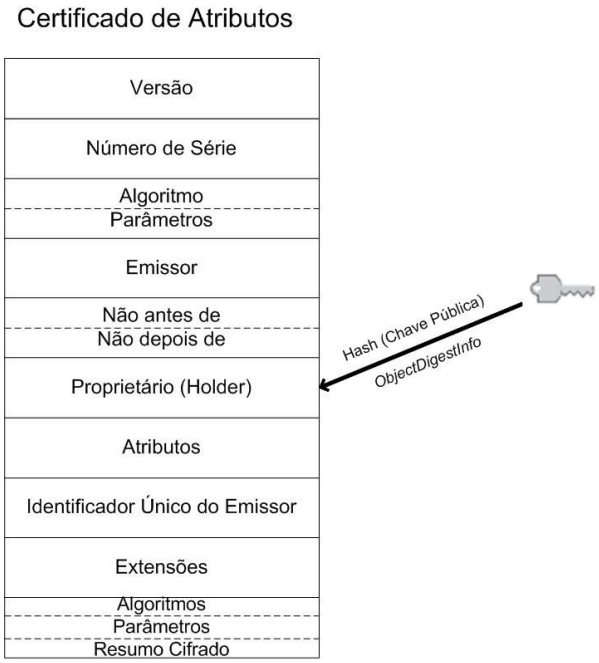

Figura 4-12 - Vínculo através da opção *ObjetctDigestInfo*

4.3.3 Emissor

O campo emissor do certificado de atributo deve utilizar a opção *v2Form*, para estar em conformidade com o padrão da referência [18]. Esta opção deve conter um e somente um *GeneralName* no subcampo *issuerName*, que deve conter um nome distinto não vazio. Isto significa que toda entidade emissora de certificados de atributo deve ter um nome distinto não vazio registrado em algum diretório. Além desses requisitos, os certificados de atributo que buscam a conformidade com o padrão da referência [18] não devem utilizar as opções *baseCertificateID* e *objetctDigestInfo* do formulário *v2Form* do campo emissor. Esses campos devem ser omitidos segundo o padrão proposto. Isso evita que o emissor do certificado de atributo tenha que saber que certificado de chave pública o verificador do certificado de atributo usará para identificá-lo.

4.3.4 Assinatura

Esse campo contém o algoritmo criptográfico utilizado para a criação da assinatura do certificado de atributo. O algoritmo escolhido deve ser um dos algoritmos de assinatura definidos na referência [19].

4.3.5 Número Serial

É de fundamental importância que a combinação de Entidade Emissora (emissor) e o número serial identifiquem unicamente qualquer certificado de atributo. Para isso, as entidades emissoras utilizar números inteiros positivos geralmente grandes no campo número serial. O tamanho desse campo, entretanto, não pode ser maior que vinte octetos.

Não há nenhuma regra definida para a geração dos números seriais. A entidade emissora deve garantir somente que os números gerados crescerão com o tempo e que todo número serial gerado é único.

4.3.6 Período de validade

O campo *AttCertValidityPeriod* do certificado de atributos define o período no qual o vínculo entre o proprietário do certificado e os atributos definidos são válidos. Em qualquer outro período, antes ou depois, os atributos especificados no certificado não são válidos para aquele proprietário.

Existem diferentes notações que podem ser usadas para designar informações de datas e horários. Visando dirimir dúvidas, nos campos *notBeforeTime* e *notAfterTime* são colocados uma representação padrão *Abstract Syntax Notation One* (ASN.1) [12]. O tipo de padrão ASN.1 utilizado é chamado *GeneralizedTime*.

A sintaxe do *GeneralizedTime* utiliza 4(quatro) dígitos para o ano, 2(dois) dígitos para o mês, dia, hora minuto e segundo, além de um campo fração de segundo. Se hão há qualquer informação adicional, a data e hora são entendidas como locais. Para indiciar uma hora em *Coordinated Universal Time* (UTC), adiciona-se uma letra Z maiúscula à representação.

Para que o certificado esteja aderente ao padrão definido na referência [18], os valores em *GeneralizedTime* devem estar expressos em *Coodinated Universal Time* (UTC), também conhecido como hora de *Greenwich*. Além disso, os segundos também devem ser expressos, mesmo que sejam iguais à zero, sem, contudo, utilizar valores fracionários.

Como exemplo, para representar a data 15 de fevereiro de 2002 no horário 17:00:10 o valor válido seria 20020515170010Z, onde o Z maiúsculo representa o horário de *Greenwich*.

Os usuários do certificado de atributo devem estar habilitados a lidar e processar corretamente certificados cujo período de validade ainda não se iniciou e também com outros cuja validade já expirou.

4.3.7 Atributos

O campo atributos fornece informações sobre o proprietário do certificado. Se o certificado é utilizado para autorização, o campo atributos contém privilégios concedidos ao proprietário sobre os objetos protegidos.

Esse campo contém uma seqüência de atributos, onde cada atributo pode conter um conjunto de valores. Para um dado certificado de atributo, cada identificador de objeto (*AttributeType*) deve ser único. Em outras palavras, um atributo deve aparecer somente uma vez no certificado, mas esse atributo pode ser atribuído a vários objetos protegidos.

Para que um certificado de atributo seja válido, o campo atributos deve ter pelo menos um atributo. A esse campo não é permitida a atribuição de uma seqüência vazia.

4.3.8 Identificador único do emissor

A utilização desse campo tem duas situações distintas:

1) Esse campo não deve ser usado, se ele não estiver sendo utilizado no certificado de chave pública do emissor do certificado de atributo;

2) Esse campo deve ser usado, se ele também for utilizado no certificado de chave pública do emissor do certificado de atributo.

As entidades, porém, devem estar habilitadas a tratar esse campo, caso ele seja utilizado ou não.

4.3.9 Extensões

Diferentemente dos campos anteriores, que fornecem informações sobre o proprietário do certificado, as extensões fornecem informações adicionais sobre o próprio certificado de atributo.

O uso de extensões é adicional. Certificados de atributo sem extensões estão de acordo com o padrão especificado na referência [18].

5. CONCLUSÃO

O estudo foi realmente efetivo para a compreensão do funcionamento de uma infra-estrutura de chave pública e também para a entender o que é e como funciona uma *Privilege Management Infrastructure* – PMI – foco da minha pesquisa de mestrado.

Nesse estudo foi possível verificar as similaridades entre ambas as infra-estruturas. Assim, pode-se entender os pontos falhos dos modelos, e possíveis soluções. Esclareceu-se também a função de um serviço de autorização e os modos de implementação, com utilização de certificados de chave pública ou com certificados de atributo.

Esse trabalho também esclareceu o termo “certificado X.509”, que em um primeiro momento nos leva a associar com certificados de chave pública. Conforme detalhado nesse relatório, o termo “certificado X.509” na verdade é um termo ambíguo, pois pode ser tanto um certificado de chave pública, usado para autenticação, quanto um certificado de atributos, usado para autorização.

6. REFERÊNCIAS

[1]. ITU-T Recommendation X.509, “Information Technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks”, 2000

[2]. C. Adams, S. Lloyd, “Understanding Public-key Infrastructure: Concepts, Standards and Deployment Considerations”, New Riders, 1999

[3]. S. Farrell, “Na Internet Attribute Certificate Profile for Authorization”, RFC3281, 2002.

[4] . D. Chadwick, “An X.509 Role-based Privilege Management Infrastructure”, Bussiness Briefing: Global Infosecurity, 2002.

[5] . E. Dawson, J. Lopez, J. A. Montenegro, “A New Design of Privilege Management Infrastructure for Organizations Using Outsourced PKI”, 2002

[6]. R. Terada, “Segurança de dados – criptografia em redes de computador”, E. Blücher, 2000.

[7]. A. Nash, W. Duane, C. Joseph, D. Brink, “PKI: Implementing and Managing E-Security”, McGraw-Hill, 2001.

[8] David F. Ferraiolo, Dennis M. Gilbert and Nickilyn Lynch. “An examination of federal and commercial access control policy needs”. In NIST-NCSC National Computer Security Conference, páginas 107-116, Baltimore, MD, Setembro 1993.

[9] R. S. Sandhu, E.J. Coyne, H.L. Feinstein, “Role-Based Access Control Models”, 1996.

[10] R. Housley, W. Polk, W. Ford, D. Solo. “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 3280, 2002.

[11] Sítio do ASN.1 Consortium, disponível em http://www.asn1.org.

[12] J. Larmouth. “ASN.1 Complete”, Morgan Kaufmann, 1999. 472 p. Disponível gratuitamente em http://www.oss.com/asn1/larmouth.html.

[13] P. Lareau. “PKI Basics - A Business Perspective”, A PKI Forum Note, 2002. Disponível em http://www.pkiforum.org/resources.html

[14] D. Brink. “PKI and Financial Return on Investment”, A PKI Forum Note, 2002. Disponível em http://www.pkiforum.org/resources.html.

[15] R. Housley, W. Polk, W. Ford, D. Solo. “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC 2459, 1999.

[16] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”, RFC 2560, 1999.

[17] C. Adams, S. Farrell. “Internet X.509 Public Key Infrastructure Certificate Management Protocols”, RFC 2510, 1999.

[18] S. Farrell, R. Housley. “An Internet Attribute Certificate Profile for Authorization”, RFC 3281, 2002.

[19] L. Bassham, W. Polk, R. Housley. “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. RFC 3279. 2002