UNIVERSIDADE DE SÃO PAULO

ESCOLA POLITÉCNICA

FÁBIO VILLAMARIN ARREBOLA

Um modelo de controle de acesso a recursos de rede baseado em Infra-estrutura de Chaves Públicas e Infra-estrutura de Gerenciamento de Privilégios

São Paulo

2006

FÁBIO VILLAMARIN ARREBOLA

Um modelo de controle de acesso a recursos de rede baseado em Infra-estrutura de Chaves Públicas e Infra-estrutura de Gerenciamento de Privilégios

Dissertação apresentada a Escola Politécnica da
Universidade de São Paulo para obtenção do título de
Mestre em Engenharia Elétrica

Área de Concentração: Sistemas Eletrônicos
Orientador: Prof. Dr. Pedro Luis Prospero Sanchez

São Paulo

2006

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 26 de julho de 2006.

Assinatura do autor _____

Assinatura do orientador _____

FICHA CATALOGRÁFICA

Villamarin Arrebola, Fábio
Um modelo de controle de acesso a recursos de rede baseado em infra-estrutura de chaves públicas e infra-estrutura de gerenciamento de privilégios / F. Villamarin Arrebola. -- ed.rev. -- São Paulo, 2006.
109 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1.Segurança de redes 2.Redes de computadores 3.Gerência de redes I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Sistemas Eletrônicos II.t.

DEDICATÓRIA

Aos meus pais, Odilthom e Ines, que sempre me incentivam em quaisquer dos objetivos almejados.

Ao meu irmão Fernando e à minha família por todo seu apoio.

À Alline, por seu carinho, compreensão, presença durante todo o período do mestrado.

Aos meus amigos, Artur, Leonardo, Murilo e Renato, que dividem comigo este longo caminho em busca do conhecimento.

AGRADECIMENTOS

Ao meu orientador, Prof. Dr. Pedro Luis Prospero Sanchez, por seu conhecimento, pela oportunidade dada, pela paciência e pelo incentivo.

Ao Dr. Volnys Borges Bernal, pela experiência, amizade e confiança depositada.

Aos amigos do Grupo NSRAV, pela ajuda e apoio em todos os momentos.

À Escola Politécnica da Universidade de São Paulo e ao Laboratório de Sistemas Integráveis por colocar a disposição sua infra-estrutura.

RESUMO

ARREBOLA, F. V. **Um modelo de controle de acesso a recursos de rede baseado em Infra-estrutura de Chaves Públicas e Infra-estrutura de Gerenciamento de Privilégios**. 2006. 111 f. Dissertação (Mestrado em Engenharia Elétrica) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2006.

A separação dos serviços de autenticação e autorização, que na recomendação X.509 é endereçada através da proposta de duas infra-estruturas distintas, a ICP e a IGP, traz grandes benefícios, já que, através dela, fatores relacionados principalmente ao âmbito administrativo podem ser tratados de forma isolada e granular. No entanto, vale observar que essa separação de serviços, embora benéfica do ponto de vista administrativo, só pode trazer resultados positivos ao âmbito da segurança se houver, entre eles, um método de interação que seja simples, modular e extensível. O principal objetivo deste trabalho é propor um modelo de interação entre as infra-estruturas X.509 ICP e IGP que seja aplicável a ambientes de rede que tenham por meta controlar o acesso a recursos. Esse modelo possibilita que aplicações que lidam com informações sensíveis façam uso, de forma integrada, tanto dos serviços de autenticação quanto dos serviços de autorização oferecidos respectivamente pelas infra-estruturas ICP e IGP. Com isso, é possível tratar a autenticação de entidades, a autorização e conseqüente controle de acesso de forma única, através de uma só arquitetura, tornando a utilização das infra-estruturas X.509 ICP e IGP ainda mais difundida e mais abrangente.

ABSTRACT

The separation between authentication and authorization services is handled by the X.509 recommendation through two distinct infrastructures, named PKI and PMI. This separation brings many benefits, since some of the elements related to the administrative area can be treated in an isolated form. Although, it is worth to point that this separation of services can only bring positive results to the security area if there's some kind of method that provides interaction between them. Also, this method shall be simple, modular and extensible. The main objective of this work is to purpose an interaction model between PKI and PMI infrastructures that can be used in a network environment that has the will of controlling access to resources. By using this model, applications that handle sensible information can use a single architecture that offers authentication and authorization services. In addition, the understanding of the concepts involved by the X.509 infrastructures can be spread out, making those technologies more used and more comprehensive.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

AA	Autoridade de Atributos (*Attribute Authority*)
AC	Autoridade Certificadora (*Certificate Authority*)
AGCA	Agente Gerenciador de Certificados de Atributos
AR	Autoridade de Registro
ASN.1	*Abstract Syntax Notation 1*
CA	Certificado de Atributos (*Attribute Certificate*)
CABP	Controle de Acesso Baseado em Papéis (*Role Based Access Control*)
CAD	Controle de Acesso Discreto (*Discretionary Access Control*)
CAM	Controle de Acesso Mandatório (*Mandatory Access Control*)
CCP	Certificado de Chave Pública (*Public Key Certificate*)
CEP	Certificado de Especificação de Papel (*Role Especification Certificate*)
CMP	*Certificate Management Protocol*

CRP	Certificado de Relacionamento a Papéis (*Role Association Certificate*)
EAP	Entidade de Atribuição de Privilégios
ECA	Entidade Controladora de Aplicações
FA	Fonte de Autoridade (*Source of Authority*)
FDCA	Função de Decisão de Controle de Acesso (*Access Control Decision Function*)
FECA	Função de Execução do Controle de Acesso (*Access Control Enforcement Function*)
HTTP	*Hypertext Transfer Protocol*
IDCA	Informação de Decisão para o Controle de Acesso (*Access Control Decision Information*)
ICA	Informações de Controle de Acesso (*Access Control Information*)
ICP	Infra-estrutura de Chaves Públicas (*Public Key Infrastructure*)
IGP	Infra-estrutura de Gerenciamento de Privilégios (*Privilege Management Infrastructure*)
ITU-T	*International Telecommunications Union, Telecommunication Standardisation Sector*

LCAR	Lista de Certificados de Atributos Revogados (*Attribute Certificate Revocation List*)
LCR	Lista de Certificados Revogados (*Certificate Revocation List*)
LDAP	*Lightweight Directory Access Protocol*
PA	Política de Autorização
PERMIS	*Privilege and Role Management Infrastructure Standards Validation*
PAC	Protocolo de Apresentação de Credenciais
PSP	Protocolo de Solicitação de Privilégios
PRIME	*Privacy and Identity Management for Europe*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
XACML	*eXtensible Access Control Markup Language*
XML	*eXtensible Markup Language*

1. INTRODUÇÃO

Ao mesmo passo em que a utilização do meio digital como forma de armazenamento de informações se torna cada vez mais presente na vida cotidiana, os ambientes corporativos, sejam eles de pequeno, médio ou grande porte, requerem que certas precauções sejam tomadas em relação à exposição das informações sensíveis. Geralmente armazenadas em servidores, essas informações, ora materializadas sob o formato de arquivos, registros em um banco de dados, ou mesmo páginas *web*, são alguns dos recursos de maior valia em algumas corporações. Portanto, restringir o acesso aos mesmos, garantindo que seu conteúdo esteja disponível apenas àqueles que possuam os privilégios necessários, bem como detectar as tentativas de violação das políticas de segurança existentes, passa a ser atividade crucial para o sucesso de uma corporação que preze pela manutenção do sigilo de suas informações.

Para que os objetivos anteriormente discutidos sejam alcançados, é fundamental a existência de mecanismos e procedimentos capazes de identificar as entidades e os privilégios a elas associados. Através de sua aplicação, os conhecidos e tão almejados objetivos da segurança da informação, identificação (ou autenticação de entidades) e autorização podem ser alcançados. Ainda assim, mecanismos capazes de tratar outros objetivos, tais como o sigilo e a integridade das informações trafegadas, ou mesmo a tempestividade e o não-repúdio das ações realizadas, também devem ser levados em consideração, uma vez que esses objetivos também podem ser considerados essenciais para a manutenção da segurança.

Em relação aos mecanismos de identificação e autorização, estes realizam suas atividades em duas etapas que, embora distintas, estão fortemente ligadas. Durante a primeira etapa, é necessário atestar-se a veracidade da identidade apresentada pelo originador de uma requisição. Em seguida, durante a segunda etapa, é necessário que se ateste se os privilégios

atribuídos à identidade apresentada na etapa anterior satisfazem as condições predeterminadas. Como exemplo para mecanismos com essa característica, pode ser citado um cenário simples, no qual as informações apresentadas pelo requisitante para a composição de sua identidade, que em seu formato mais comum são determinadas por uma combinação válida de nome de usuário e senha, servem de base para o esquema de controle de acesso.

Entretanto, vale observar que tanto a autenticação de entidades quanto a autorização não se resumem a isso. Inúmeras são as técnicas disponíveis, desde as mais simples até as mais elaboradas. Muitas delas, em especial as que utilizam listas para o armazenamento das informações, quando aplicadas a ambientes distribuídos, podem ocasionar diversos problemas relacionados à administração. Em ambientes como esse, nos quais a freqüência de mudanças é geralmente considerável, manter as inúmeras listas devidamente atualizadas, bem como garantir sua concordância com as políticas de segurança existentes, são algumas das questões que dão origem ao grande fardo da administração quando o assunto é manter o sigilo de informações sensíveis: o gerenciamento.

Buscando contornar o obstáculo administrativo, diversas alternativas foram propostas ao longo do tempo. Dentre elas, encontram-se algumas técnicas que, devido ao fato de basearem seu funcionamento na utilização de certificados digitais, merecem atenção especial para os objetivos deste trabalho. Em relação à autenticação, a recomendação X.509 do *International Telecommunication Union - Telecommunication Standardisation Sector* (ITU-T), encontrada em (ITU-T, 2000) e também publicada como padrão internacional ISO/IEC, sob o número 9594-8, define a Infra-estrutura de Chaves Públicas (ICP); um arcabouço de distribuição segura de informações entre as entidades pertencentes a um domínio. Baseado em técnicas de criptografia de chave pública, o arcabouço ICP, atualmente uma das opções mais difundidas para fins de autenticação, também pode ser utilizado com o objetivo de manter o sigilo e a integridade das informações trafegadas. Já em relação à autorização, a mesma

recomendação X.509 define a Infra-estrutura de Gerenciamento de Privilégios (IGP), um arcabouço que, ao atuar opcionalmente em conjunto com uma ICP, visa distribuir e gerenciar privilégios entre as entidades pertencentes a um domínio.

Alicerce de diversos projetos bem-sucedidos, a IGP e sua utilização como esquema de suporte a aplicações que requeiram funcionalidades de autorização baseadas em certificados digitais são pouco difundidas. Para justificar essa afirmação, os argumentos mais utilizados baseiam-se na suposta complexidade de implantação, desempenho e, principalmente, na dependência de uma ICP. Dessa forma, quando o assunto se volta sobre a integração entre os arcabouços definidos na recomendação X.509, poucas iniciativas podem ser citadas. E cada vez mais, trabalhos focados no controle de acesso a recursos em ambientes com freqüência de mudanças considerável tornam visível a necessidade por um modelo simples e padronizado capaz de prover serviços de autenticação e autorização às aplicações que lidam com informações sensíveis.

1.1. MOTIVAÇÕES

A separação dos serviços de autenticação e autorização, que na recomendação X.509 é endereçada através da proposta de duas infra-estruturas distintas, a ICP e a IGP, traz grandes benefícios, já que, através dela, fatores relacionados principalmente ao âmbito administrativo podem ser tratados de forma isolada e granular. No entanto, vale observar que essa separação de serviços, embora benéfica do ponto de vista administrativo, só pode trazer resultados positivos ao âmbito da segurança se houver entre eles um método de interação que seja simples, modular, extensível e baseado em padrões.

Prevista na recomendação X.509, essa necessidade se reflete no próprio formato dos

certificados pertencentes à infra-estrutura IGP. Por não armazenarem informações referentes às identidades dos sujeitos para os quais foram emitidos, esses certificados estabelecem, através de um identificador flexível, um vínculo com certificados capazes de fazê-lo. Entretanto, esse identificador, ainda que capaz de viabilizar o relacionamento entre as infra-estruturas ICP e IGP, não prevê como a interação entre ambas deve tomar parte.

Dessa forma, no que se refere à recomendação X.509, fazer com que as infra-estruturas nela encontradas interajam, de forma a capacitar as aplicações que lidam com informações sensíveis a utilizar os serviços de segurança por elas proporcionados, é o grande motivador desse trabalho. Através dessa interação, uma série de objetivos da segurança da informação, tais como a autenticação de entidades, a autorização e até mesmo a auditoria, pode ser endereçada de forma única, tornando a utilização das infra-estruturas X.509 ICP e IGP ainda mais difundida e mais abrangente.

1.2. OBJETIVOS

O principal objetivo deste trabalho é propor, implementar e analisar um modelo de interação entre as infra-estruturas X.509 ICP e IGP que seja aplicável a ambientes de rede que tenham por meta controlar o acesso a recursos de rede. Esse modelo possibilita que aplicações que lidam com informações sensíveis façam uso, de forma integrada, tanto dos serviços de autenticação quanto dos serviços de autorização oferecidos respectivamente pelas infra-estruturas ICP e IGP. Outros serviços de segurança, tais como a tempestividade, o não-repúdio e a auditoria das ações realizadas, também são alvos dessa integração, visto que eles podem ser considerados fundamentais na concretização de diversos objetivos relacionados à segurança da informação, incluindo reconstrução de eventos e detecção de intrusão.

1.3. METODOLOGIA

Para que os objetivos anteriormente discutidos fossem alcançados, procurou-se realizar, inicialmente, um levantamento bibliográfico referente à utilização de certificados digitais no endereçamento de questões relacionadas à autenticação e, principalmente, à autorização.

No que se refere à autenticação, o levantamento do estado da arte resultou no conhecimento, através da recomendação X.509 (ITU-T, 2000), da ICP, uma infra-estrutura de gerenciamento de certificados de chave pública que está na lista das técnicas de autenticação mais utilizadas atualmente. Após o estudo detalhado de suas características e de outras recomendações relacionadas, como, por exemplo, os protocolos de gerenciamento de certificados (ADAMS et al, 2005), a atenção se voltou para as tecnologias de autorização existentes.

Por intermédio dessa pesquisa, tomou-se conhecimento, ainda através da recomendação X.509, da existência da IGP, uma infra-estrutura de gerenciamento de privilégios que baseia seu funcionamento nos conceitos de certificado digital e que pode, em caráter opcional, interagir com uma ICP. Na tentativa de melhor compreender seu funcionamento, foi possível perceber que, antes de qualquer coisa, era necessário que se buscasse pelos métodos de controle de acesso tradicionais. Embora a IGP estivesse estritamente relacionada com a ICP, estudar os modelos de controle de acesso baseados em listas, tais como o modelo de Controle de Acesso Discreto (CAD), era fundamental. Encontrado em National Computer Security Center (2003), o CAD, ou *Discretionary Access Control*, tem como característica principal a associação direta entre privilégios e objetos.

Em seguida, outros modelos de controle de acesso puderam ser conhecidos. Dentre

eles, um merece atenção especial visto sua utilização em um dos mais importantes trabalhos relacionados. Proposto em Ferraiolo e Kuhn (1992), o modelo de Controle de Acesso Baseado em Papéis (CABP), ou *Role Based Access Control*, diferentemente do CAD, associa privilégios a papéis e papéis a entidades. Dessa forma, a associação entre entidades e privilégios é feita de forma indireta.

Continuando o levantamento do estado da arte para os modelos de autorização de acesso, voltou-se a atenção para as técnicas de gerenciamento e distribuição de privilégios. Agora, sim, era a vez do estudo detalhado das características da IGP. E, em busca de trabalhos que utilizassem tal tecnologia, foi possível encontrar um exemplar de grande importância para a essência deste trabalho: o projeto *Privilege and Role Management Infrastructure Standards Validation* (PERMIS), apresentado por Chadwick e Otenko (2002a).

Utilizando o modelo CABP e políticas bem flexíveis, o PERMIS tem por objetivo validar a utilização de certificados digitais de atributo no contexto do controle de acesso a recursos. Ao aprofundar-se a análise de suas características principais, em destaque os relacionamentos com mecanismos de autenticação, o foco da pesquisa voltou-se sobre a interação entre as infra-estruturas X.509 ICP e IGP. Trabalhos centrados principalmente no campo da medicina, categoria na qual se enquadram as iniciativas de Wohlmacher e Pharow (2000), de Blobel et al (2003), e até mesmo o trabalho de Polemi, Hoepner e Bourka (2000), além de ressaltar as poucas iniciativas que podem ser citadas sobre o assunto, tornam visível a necessidade por um modelo capaz de prover serviços de autenticação e autorização às aplicações de rede que lidam com informações sensíveis.

Após a identificação dessa necessidade, um modelo de interação entre as infra-estruturas X.509 foi projetado, discutido e implementado. Esse modelo, explicado em detalhes no capítulo 6, é formado, em resumo, por dois elementos: a Entidade Controladora de Aplicações (ECA) e o Agente Gerenciador de Certificados de Atributos (AGCA). A ECA é

responsável, entre outras tarefas, por restringir o acesso aos recursos protegidos de rede através da validação do contexto de uma requisição de acesso. A validação do contexto envolve, entre outras, as informações apresentadas pelo usuário final. Essa validação, que em parte representa a interação entre as infra-estruturas X.509 ICP e IGP, pode ser traduzida na verificação de algumas das propriedades dos certificados digitais, como, por exemplo, a revogação. Já o AGCA deve, além de trocar informações com a própria ECA, interagir com o cliente final, solicitando quais certificados devem ser considerados.

1.4. TRABALHOS CORRELATOS

Há, na literatura, uma série de trabalhos referentes à utilização de certificados digitais para controlar acesso a recursos, entre eles o *Akenti* (JOHNSTON; MUDUMBAI; THOMPSON, 1998) e o *Shibboleth* (CANTOR; ERDOS, 2005). Em resumo, o *Akenti* tem como principal objetivo fornecer um modelo que permita o gerenciamento distribuído de recursos, ou seja, permitir que múltiplas partes gerenciem, de forma simultânea, um único recurso. Já o *Shibboleth* tem como foco principal suportar a autenticação e a autorização entre instituições, protegendo a privacidade do usuário através do uso de pseudônimos. Para isso, visa construir uma arquitetura para uma infra-estrutura de controle de acesso a recursos *web* que, além de se basear nos padrões existentes e ser independente de plataforma, possa operar através de limites institucionais.

Ainda em relação aos exemplos de trabalhos centrados no controle de acesso, até mesmo a recente iniciativa *Privacy and Identity Management for Europe* (PRIME) (PRIME Consortium, 2005) pode ser citada. No entanto, mesmo em meio a essa diversidade de exemplos, apenas um trabalho, por ter sido a base para o modelo proposto nesta dissertação,

será discutido aqui: o PERMIS (CHADWICK; OTENKO, 2002a), discutido com detalhes no capítulo 5. Sua importância está relacionada, entre outras coisas, ao fato de que sua proposta é uma das primeiras que se utilizam amplamente dos padrões existentes. Como comparação, basta considerar-se o projeto *Akenti*. Ambos os trabalhos possuem arquiteturas semelhantes, porém, enquanto o PERMIS constrói suas credenciais em concordância com o padrão X.509, o *Akenti* se utiliza de um formato proprietário especificado sob a sintaxe *eXtensible Markup Language* (XML). Além disso, o mecanismo de verificação de privilégios do PERMIS baseia-se no arcabouço geral de controle de acesso encontrado na recomendação X.812 (ITU-T, 1995).

O objetivo principal do PERMIS, segundo Chadwick, Otenko e Ball (2003), é mostrar que os conceitos envolvidos na definição da IGP podem ser usados para construir uma infra-estrutura de gerenciamento de confiança que, utilizando o modelo de controle de acesso baseado em papéis (CABP), seja fundamentada pelas definições dadas por Blaze, Feigenbaum e Ioannidis (1999). De acordo com esse trabalho, uma infra-estrutura de gerenciamento de confiança é formada por cinco componentes:

- uma linguagem que descreve as ações a serem controladas;
- um mecanismo que identifica os sujeitos (entidade final) autorizados a realizar ações;
- uma linguagem que especifica as políticas de segurança que governam as ações;
- um mecanismo que especifica as credenciais e possibilita, entre outras coisas, que as entidades finais deleguem seus privilégios a outras entidades;
- um mecanismo verificador de conformidade, responsável por determinar como as ações iniciadas pelas entidades finais devem ser tratadas, sempre levando em consideração um conjunto de credenciais e uma política de segurança.

Entretanto, como pode ser observado no próprio trabalho de Chadwick, Otenko e Ball (2003), tanto o estudo das características da IGP, quanto das infra-estruturas de gerenciamento de confiança levaram à identificação de algumas necessidades. Com isso, as contribuições mais significantes do projeto se relacionam à definição das ações e políticas de segurança e também à construção do mecanismo verificador de conformidade. Em adição, outro componente, considerado por Chadwick, Otenko e Ball (2003) como elemento essencial para um sistema completamente funcional, e não mencionado explicitamente pelos trabalhos ITU-T (2000) e Blaze, Feigenbaum e Ioannidis (1999), deve ser levado em consideração: o subsistema de alocação de privilégios, que permite ao emissor de credenciais o gerenciamento dos privilégios associados às entidades.

1.5. ORGANIZAÇÃO DO TRABALHO

A dissertação está organizada em sete capítulos dispostos de forma a posicionar o leitor frente à teoria envolvida nas tecnologias aqui utilizadas. O capítulo 2 visa, inicialmente, proporcionar ao leitor conhecimento básico sobre os conceitos de uma ICP: entidades e estruturas envolvidas na emissão e gerenciamento de certificados digitais de chave pública. Em seguida, são discutidas as questões relacionadas ao uso da ICP para fins de autorização.

O controle de acesso é o assunto discutido durante o terceiro capítulo da dissertação. Nele, são apresentados os modelos tradicionais de controle de acesso a recursos e as modalidades de distribuição de credenciais. Além disso, é feita uma comparação entre tais modalidades, elucidando prós e contras de cada uma delas. Devido à sua utilização no trabalho relacionado PERMIS, é discutido, ainda durante o terceiro capítulo, o arcabouço geral de controle de acesso definido na recomendação X.812 (ITU-T, 1995).

Durante o capítulo 4, é abordada a infra-estrutura de gerenciamento de privilégios IGP, destacando-se as entidades e estruturas envolvidas na emissão e gerenciamento de certificados digitais de atributo. Além disso, são discutidos os modelos de funcionamento e os relacionamentos da IGP com a ICP.

Tendo como base os modelos de controle de acesso discutidos durante o terceiro capítulo e também os conceitos relacionados à IGP, o quinto capítulo tem por objetivo discutir o trabalho relacionado PERMIS. Em seguida, durante o capítulo 6, o modelo aqui proposto será apresentado, discutindo-se seus elementos e formas de operação.

O capítulo 7 apresentará as considerações finais sobre o modelo proposto. Além de formular as conclusões, esse capítulo visa também apontar as possíveis extensões deste trabalho.

Por fim, existe um anexo que descreve os conceitos básicos sobre criptografia, úteis para a compreensão das tecnologias de certificados digitais abordadas durante o transcorrer da dissertação.

2. A INFRA-ESTRUTURA DE CHAVES PÚBLICAS

Segundo Menezes, Oorscho e Vanstose (1996), no meio digital, proteger a informação sensível requer que uma série de objetivos relacionados à segurança da informação seja alcançada, entre eles o sigilo e a integridade. Enquanto aquele visa garantir que a informação sensível esteja disponível apenas aos que possuam os privilégios necessários, este tem como finalidade assegurar que não haja modificações indevidas em seu conteúdo.

Além do sigilo e da integridade, há outro objetivo que merece atenção especial. Ao proporcionar vínculos suficientes entre a identidade que uma parte declara e aquilo que ela realmente é, a identificação, ou autenticação de entidades, visa tratar uma das mais importantes questões relacionadas à segurança da informação no meio digital: a personificação.

Para endereçar os objetivos anteriormente descritos, é comum a utilização de técnicas de criptografia de chave pública (detalhada no Apêndice A). Conforme Burnett e Paine (2001), essa modalidade de criptografia não oferece apenas um poderoso mecanismo de manutenção do sigilo das informações, mas também uma maneira de identificar outras entidades. Porém, para que isso seja possível, alguns problemas inerentes à própria criptografia de chave pública, relacionados principalmente à eficácia do gerenciamento e à distribuição de chaves em ambientes distribuídos, devem ser solucionados.

Tal tarefa não seria tão dispendiosa se houvesse apenas pequenas populações de usuários confiáveis. Entretanto, a realidade mostra que, em ampla escala, faz-se necessário um método escalonável e sistemático (BURNETT; PAINE, 2001). Sendo assim, da necessidade de distribuição de chaves nasceu o Certificado de Chave Pública (CCP). Também denominado *Public Key Certificate*, esse certificado representa uma estrutura capaz de

assegurar a relação entre uma chave pública e uma identidade.

Amplamente discutidos no meio acadêmico, e cada vez mais adotados no âmbito comercial, os certificados digitais de chave pública e os conceitos que a eles se relacionam deram origem à necessidade de procedimentos que possibilitassem um gerenciamento de certificados eficaz. Essa necessidade implicou na criação de um conjunto de políticas e procedimentos necessários para gerenciar, armazenar, distribuir e revogar certificados. Ao adicionar a este conjunto componentes de hardware e software, bem como o elemento humano, surgiu a Infra-estrutura de Chaves Públicas (ICP).

Alguns autores, entre eles Binder (2004), definem a ICP, também chamada de *Public Key Infrastructure*, como um sistema de suporte às assinaturas digitais e à manutenção do sigilo de documentos em uma organização. Entretanto, é importante enfatizar que a ICP tem um objetivo mais amplo: o de prover um arcabouço de segurança para todas as aplicações que utilizem certificados digitais. Com esse arcabouço é possível atender a uma série de requisitos de segurança, entre eles o sigilo, a integridade e o não-repúdio.

2.1. COMPONENTES

Em seu modelo arquitetural tradicional, ilustrado na Figura 1, a ICP, além de definir a estrutura das informações armazenadas pelos certificados, define as entidades e o papel que cada uma delas deve exercer. Em suma, esse modelo, baseado na descrição existente em Burr et al (2004), é representado pelas entidades finais, entidades registradoras e emissoras de certificados, além de todas as outras entidades necessárias para suportar operações normais que utilizem certificados digitais.

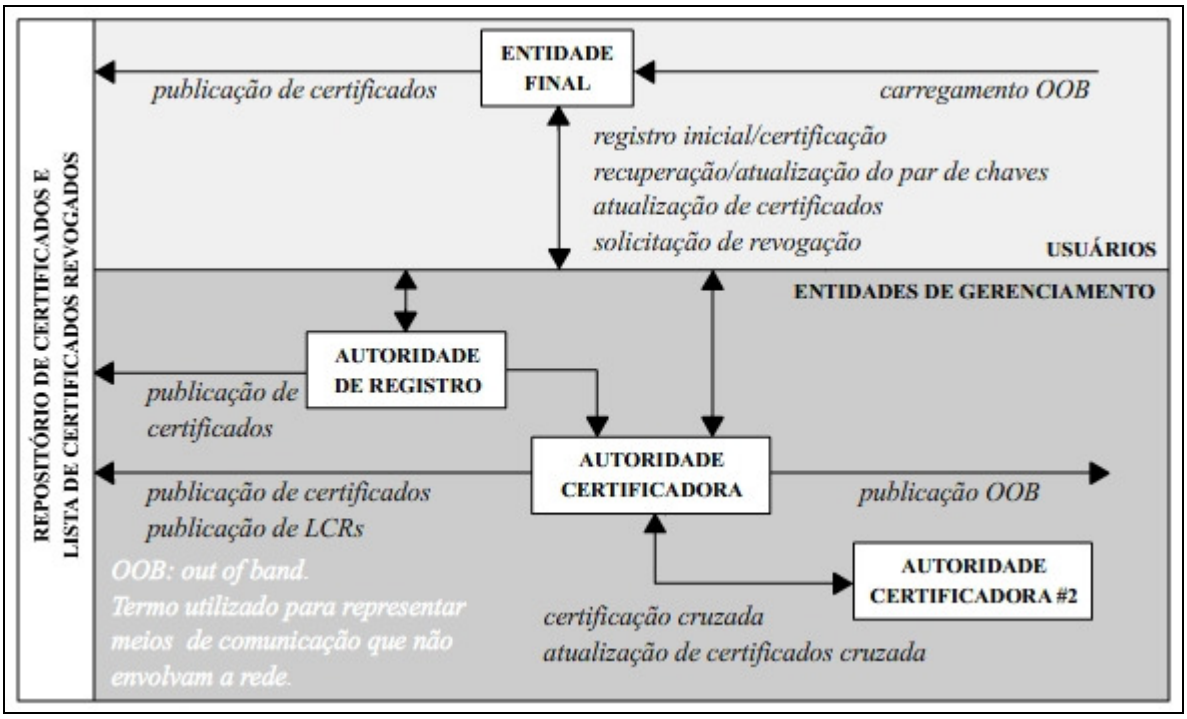

Figura 1. Modelo arquitetural de uma ICP, adaptado de Housley et al (2002).

As entidades presentes em uma ICP são as seguintes:

- **Entidade Final**. Termo utilizado para designar usuários finais, ou seja, qualquer entidade que pode ser identificada como o sujeito para o qual um certificado de chave pública tenha sido emitido.

- **Autoridade Certificadora (AC)**. Muitas vezes denominada 'terceiro confiável', esta entidade é o elemento responsável pela emissão, gerenciamento e revogação de certificados digitais. Também sob sua responsabilidade, há um outro elemento importante para o bom funcionamento de uma ICP. A Lista de Certificados Revogados (LCR) [1] é uma estrutura assinada digitalmente que tem por objetivo

[1] Observa-se que a utilização de Listas de Certificados Revogados é apenas um dos meios existentes para a verificação do estado de um certificado no que se refere à revogação. Outros meios podem ser utilizados, como, por exemplo, os protocolos de verificação *on-line* (MYERS et al, 1999).

listar os certificados inválidos sob responsabilidade da AC. A AC também pode dar suporte a várias tarefas administrativas, embora estas sejam geralmente delegadas a uma outra entidade denominada Autoridade de Registro.

- **Autoridade de Registro (AR)**. Este é um componente opcional na arquitetura de uma ICP e, conforme dito anteriormente, pode assumir algumas funções administrativas da AC, como, por exemplo, o processo de registro de entidades finais ou mesmo gerenciamento de solicitações de revogação.

- **Repositório**. Definido como um meio de armazenamento e distribuição de certificados e listas de certificados revogados, este elemento constitui a localização central das informações de entidades finais de um domínio. Embora não haja nenhum padrão requerido, o X.500 (ITU-T, 2001) tem sido amplamente aceito devido ao fato de proporcionar interoperabilidade e, principalmente, devido a um de seus protocolos de acesso: o *Lightweight Directory Access Protocol* (LDAP). Encontrado em Yeong, Howes e Kille (1995), o LDAP permite a localização de informações de forma mais simples do que o protocolo padrão X.500.

Por ajudar na comunicação entre entidades, os protocolos de gerenciamento, que incluem, por exemplo, os Protocolos de Gerenciamento de Certificados, ou *Certificate Management Protocols* (CMP) [2], formam outro elemento de grande importância para o bom funcionamento de uma ICP. Através desses protocolos são definidos os formatos das mensagens que devem ser trocadas entre entidades para que se realize uma série de tarefas administrativas que variam desde a solicitação de emissão de certificados até a notificação de

[2] A especificação completa do formato das mensagens, bem como a lista de operações de gerenciamento suportadas, pode ser encontrada em Adams et al (2005).

comprometimento de uma chave.

2.2. CERTIFICADO DE CHAVE PÚBLICA

Desde sua versão inicial, o formato do certificado de chave pública definido pelo padrão X.509 evoluiu muito, sempre em busca de maior flexibilidade. Ao armazenar as informações em uma estrutura assinada digitalmente por seu emissor, esse tipo de certificado assegura que a integridade das informações disponibilizadas foi mantida. Além disso, assegura a veracidade da ligação dessa chave a um determinado conjunto de dados que representam uma identidade.

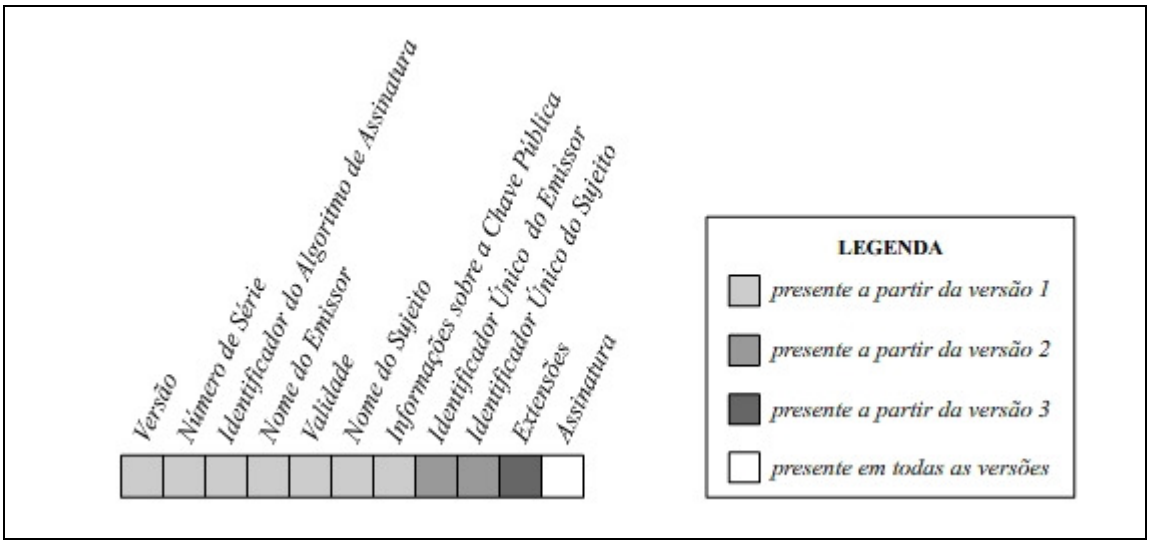

Figura 2. Estrutura do Certificado de Chave Pública X.509.

Representado na Figura 2, o certificado digital de chave pública é formado pelos

seguintes campos[3]:

- `Versão`. Campo responsável por diferenciar as sucessivas versões do certificado;
- `Número de Série`. Aqui, tem-se um identificador numérico único dentro de um domínio. Este identificador é atribuído pela entidade especificada no campo `Nome do Emissor`;
- `Identificador do Algoritmo de Assinatura`. Especifica o identificador do algoritmo utilizado para assinar digitalmente a estrutura;
- `Nome do Emissor`. Tem-se neste campo um conjunto de caracteres que identifica a entidade emissora do certificado; aquele que assinou digitalmente a estrutura;
- `Validade`. Define o intervalo de tempo durante o qual o emissor do certificado atesta, inicialmente, sua validade;
- `Nome do Sujeito`. Este campo é responsável por identificar a entidade final à qual o certificado se refere, ou seja, a entidade que mantém a chave privada correspondente à chave encontrada no campo `Informação sobre a Chave Pública`;
- `Informação sobre a Chave Pública`. Contém a chave pública da entidade final (sujeito), o identificador do algoritmo utilizado e quaisquer outros parâmetros associados;
- `Identificador Único do Emissor` e `Identificador Único do Sujeito`. Caso haja reutilização de nomes, esses campos servem como

[3] Observa-se que esse trabalho não adota a nomenclatura original para os campos pertencentes ao certificado de chave pública encontrada na recomendação X.509 (ITU-T, 2000). Há uma adaptação para a língua portuguesa.

identificadores únicos para emissor e sujeito, respectivamente. De acordo com Housley et al (2002), o uso desses campos não é recomendado;

- `Extensões`. Presente na especificação a partir da versão 3, esse campo proporciona um método adicional de associação entre atributos e entidades finais. Cada uma dessas associações adicionais, denominada extensão, é formada por conjunto de informações que determinam, além de seu valor, seu tipo e sua importância. Um dos mais notórios exemplos de extensão é o propósito da chave, ou *key usage*. Através dele uma AC pode impor restrições ao uso dos certificados emitidos.

2.3. USO DAS EXTENSÕES PARA FINS DE AUTORIZAÇÃO

Conforme descrito na recomendação X.509, é possível, através do campo `Extensões`, adicionar novos atributos à estrutura básica de um certificado de chave pública sem que modificações à notação original se façam necessárias. Essa flexibilidade faz com que essas extensões possam ser utilizadas por inúmeras aplicações, desde o armazenamento de logotipos e áudio, conforme observado em Santesson, Housley e Freeman (2004), até o armazenamento de atributos de autorização.

Certificados de chave pública podem, portanto, proporcionar serviços de autorização de forma direta, com a ressalva de que os privilégios sejam associados aos sujeitos através de práticas da própria AC (ITU-T, 2000). Isso significa que, para que um CCP seja utilizado para fins de autorização, é preciso que a associação de privilégios às entidades finais seja uma responsabilidade da AC. Para isso, deve ser utilizada a extensão `subjectDirectoryAttributes`, representada na Figura 3 através da notação *Abstract*

Syntax Notation 1 (ASN.1).

```
subjectDirectoryAttributes EXTENSION ::= {
    SYNTAX AttributesSyntax
    IDENTIFIED BY id-ce-subjectDirectoryAttributes
}

AttributesSyntax ::= SEQUENCE SIZE (1..MAX) OF Attribute

id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER ::= {id-ce 9}
```

Figura 3. Extensão subjectDirectoryAttributes.

Porém, vale observar que o uso de extensões nem sempre pode ser considerado como a solução definitiva. Associar atributos de autorização a certificados de chave pública pode dar origem a uma série de problemas.

Primeiramente, deve-se considerar o tempo de vida útil da associação entre atributos de autorização e entidades. Na grande maioria das vezes, esse intervalo de tempo é significativamente inferior à duração das relações proporcionadas pelo certificado de chave pública (WOHLMACHER; PHAROW, 2000). Com isso, situações indesejáveis podem ocorrer: certificados de chave pública com tempo de vida menor que o esperado ou, concessões de autorização com duração maior do que o desejado.

Em segundo lugar, a AC, autoridade responsável por emitir certificados de chave pública, nem sempre é a mesma autoridade responsável por atribuir privilégios às entidades. Dessa forma, tanto para a entidade emissora de certificados quanto para as entidades verificadoras, são necessários passos adicionais para a validação dos privilégios (BENJUMEA et al, 2004).

Em terceiro lugar, nem sempre uma entidade possui privilégios oriundos de uma mesma fonte (CHANG-JI; JIAN-PING; HAI-XIN, 2003). Há a possibilidade de que uma entidade possua uma série de privilégios e cada um deles seja de responsabilidade de autoridades diferentes.

Finalmente, visto que ITU-T (2000) define que um único campo seja utilizado para o armazenamento de todos os atributos de autorização (vide Figura 3), a delegação, caso permitida, deve-se aplicar igualmente a todos os atributos presentes no certificado. No entanto, pode haver diferenças entre o privilégio original e entre o privilégio delegado (CHANG-JI; JIAN-PING; HAI-XIN, 2003).

Os pontos anteriormente apresentados levam à conclusão de que, no âmbito dos certificados digitais, a melhor opção é separar as informações de autenticação das informações de autorização. Com isso, o gerenciamento dessas informações pode ser tratado mais facilmente: as concessões de privilégios às entidades podem ser administradas sem influir na validade dos certificados de chave pública. É dentro desse contexto, o de separação das informações de autenticação e de autorização, que surge o Certificado de Atributos (CA). E, para o gerenciamento de certificados desse tipo, de forma análoga à ICP, surge uma nova infra-estrutura, a Infra-estrutura de Gerenciamento de Privilégios (IGP), explicada em detalhes no capítulo 4.

3. CONTROLE DE ACESSO

Sandhu e Samarati (1994) definem controle de acesso como o ato de limitar as operações que podem ser realizadas por uma entidade sobre um determinado recurso. Com ele, objetivos da segurança da informação, como sigilo e integridade, podem ser alcançados, prevenindo a exposição e a modificação não autorizada da informação sensível. No entanto, vale observar que o controle de acesso não pode ser considerado como a solução definitiva para as questões de segurança. Sua utilização é proveitosa apenas se houver a cooperação dos serviços de autenticação, autorização e auditoria. Para ilustrar essa afirmação, basta observar-se a Figura 4, extraída do próprio trabalho de Sandhu e Samarati (1994).

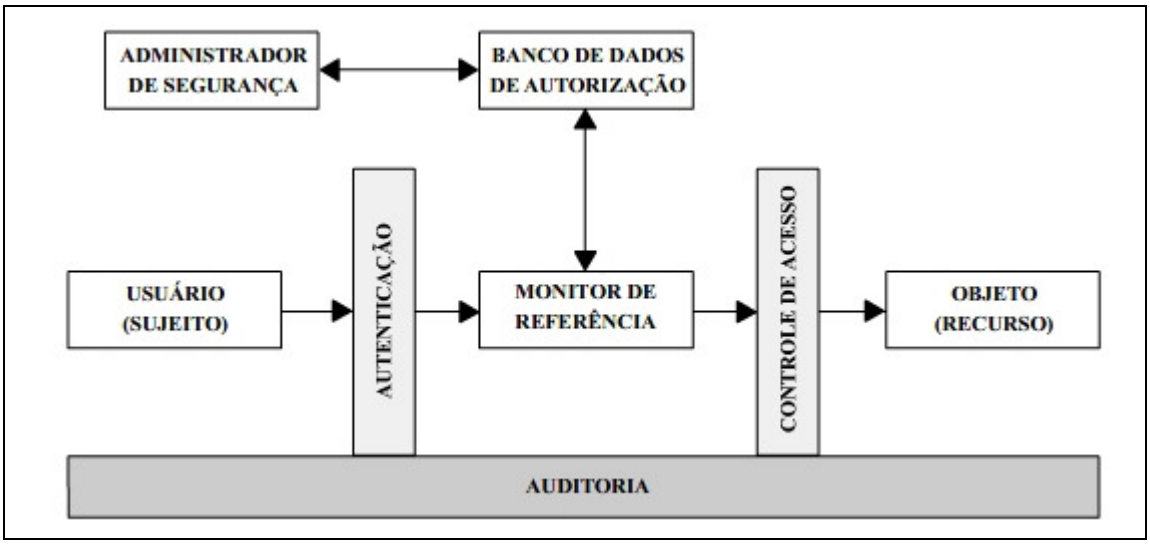

Figura 4. Controle de acesso e outros serviços de segurança, adaptado de Sandhu e Samarati (1994).

Para que um esquema de controle de acesso seja eficaz, um dos primeiros passos a ser considerado é, usualmente, a autenticação (SEIGNEUR et al, 2003). Com ela, é possível identificar as entidades finais (sujeitos) e, conforme visto no capítulo 2, tratar as questões relacionadas à personificação. Enquanto isso, e ao longo de todo o processo de concessão de

acesso, a auditoria, ao manter registros das atividades que tomaram parte, ajuda não só a detectar as violações de segurança, mas também a desencorajar as ações ilícitas. Na verdade, Motta (2003) ressalta que, no acesso a prontuários médicos eletrônicos, a ciência da realização contínua de análises dos registros de auditoria atua como forte inibidora para o uso indevido das informações.

Ainda em relação à Figura 4, pode-se observar um elemento que, embora não tenha sido citado até o momento, é de grande importância para o controle de acesso. Ao interceptar e inspecionar as requisições de acesso, o monitor de referência (também denominado mecanismo de execução) é, com o auxílio do serviço de autorização, o mecanismo responsável pela execução do controle de acesso em si. O grau de importância é tamanho que, segundo Saltzer e Schroeder (2005), uma propriedade que deve ser considerada em um mecanismo de execução é o princípio da mediação completa, ou seja, o mecanismo de execução deve estar apto a interceptar e potencialmente prevenir todo o acesso a recursos. Se for possível contorná-lo, a segurança a ser oferecida é nula.

Para determinar como o acesso deve ser controlado e como as decisões devem ser tomadas, existem as políticas de segurança que, sendo assim, regem o modo de operação dos mecanismos de execução. Divididas em três categorias principais, cada qual com características em particular, essas políticas são incorporadas pelos modelos de controle de acesso discutidos na seção a seguir. Sejam discretas, mandatárias ou mesmo baseadas em papéis, as políticas não devem ser escolhidas de acordo com sua importância, até mesmo porque, segundo Sandhu e Samarati (1994), não há, em geral, políticas melhores do que outras, mas sim políticas mais adequadas às necessidades do ambiente a ser protegido. Políticas muito restritivas, por exemplo, consideradas cruciais em alguns sistemas, podem ser inapropriadas para ambientes que requeiram maior flexibilidade.

3.1. MODELOS DE CONTROLE DE ACESSO

Os modelos de controle de acesso englobam todos os elementos necessários para que as operações de concessão de acesso se efetuem de forma adequada. Alguns desses elementos estão diretamente relacionados aos formatos através dos quais os sujeitos, os objetos e os acessos são representados. Além de estabelecer esses formatos, os modelos de controle de acesso, conforme visto anteriormente, também definem as políticas de segurança que, em outras palavras, podem ser entendidas como as regras de operação do modelo.

Hoje, há três principais modelos de controle de acesso em uso: o Controle de Acesso Discreto (CAD), o Controle de Acesso Mandatório (CAM) e o Controle de Acesso Baseado em Papéis (CABP). Outros modelos, como aqueles encontrados em Bertino et al (1998) e Joshi et al (2005), também podem ser citados. No entanto, esses modelos, no que se refere à utilização, ainda não se consolidaram, e por isso não serão abordados neste trabalho.

3.1.1. Controle de Acesso Discreto

Originado em meio a pesquisas acadêmicas, o modelo de controle de acesso discreto (CAD) tem como principal referência o trabalho de Lampson (1971). Atualmente, o CAD é um dos modelos de controle de acesso mais utilizados em ambientes computacionais.

Segundo Department of Defense (1985), o CAD, também denominado *Discretionary Access Control*, pode ser definido como um meio de restringir acesso a recursos que baseia suas decisões na identidade de um sujeito. Dessa forma, durante uma requisição de acesso, é necessário, antes que as decisões de concessão sejam tomadas, que se obtenham informações

relacionadas às identidades dos sujeitos, ou ainda, aos grupos aos quais estes pertencem.

Uma das características principais do modelo discreto está relacionada ao modo com que as permissões de acesso são gerenciadas. O acesso a um recurso pode ser autorizado apenas pelos seus proprietários. Não há gerenciamento centralizado. Além disso, a propriedade sobre um recurso pode ser transferida para outro sujeito qualquer, até mesmo de forma indireta (DEPARTMENT OF DEFENSE, 1985).

Conforme Sandhu e Samarati (1994), uma das fraquezas inerentes ao modelo CAD está relacionada ao fato de que suas políticas não impõem restrições ao uso da informação. Não há controles sobre a disseminação da informação (SANDHU; SAMARATI, 1994). Além disso, o CAD possui outras peculiaridades, como pode ser observado em Griffiths e Wade (1976) e Fagin (1978). Devido a essas e a outras sutilezas, o CAD não conseguiu grande aceitação no meio militar. Como solução, um outro modelo de controle de acesso muito mais restritivo foi proposto: o Controle de Acesso Mandatório (CAM), também denominado *Mandatory Access Control*.

3.1.2. Controle de Acesso Mandatório

O modelo de controle de acesso CAM, que surgiu como solução para algumas das fraquezas inerentes ao CAD, tem como exemplo principal a política de múltiplos níveis de segurança formalizada por Bell e Lapadula (1973), e mais tarde retomada por Sandhu (1993).

Nesse modelo, o acesso a objetos é baseado em dois fatores. Inicialmente, tem-se o grau de sensibilidade do objeto a ser acessado, também conhecido como classificação de segurança. Em seguida, tem-se o grau de autorização dos sujeitos. Ambas as informações são representadas por rótulos de segurança que, de acordo com a política utilizada, assumem

valores diferentes. Por exemplo: a política de segurança definida em Bell e Lapadula (1973) tem como objetivo principal manter o sigilo das informações, e para tal, expressa que os possíveis valores para os rótulos de segurança são: ultra-secreto, secreto, confidencial, e público. Outras políticas de segurança, tais como a encontrada em Biba (1976), definem rótulos diferentes. O objetivo principal em Biba (1976) não é zelar pelo sigilo das informações, mas sim pela sua integridade.

Em relação a suas características, vale ressaltar que o CAM, ao contrário do que ocorre no CAD, permite que apenas os administradores dos objetos, não seus proprietários, modifiquem os rótulos de segurança. No que se refere à utilização, vale ressaltar que o CAM, embora seja um modelo amplamente aceito no meio militar, tornou-se inapropriado para outras aplicações, incluindo organizações comerciais (BECKER, 2005). Isso se deve ao fato de que o CAM, além de possuir um modelo de gerenciamento estritamente rígido, possui políticas de segurança comumente muito restritivas e de pouca flexibilidade.

3.1.3. Controle de Acesso Baseado em Papéis

Embora os modelos de controle de acesso anteriormente listados sejam os mais utilizados, nem sempre eles atendem aos requisitos de algumas organizações. Um dos problemas mais desafiadores no contexto de controle de acesso a recursos é, sem dúvida, seu gerenciamento. Introduzido por Ferraiolo e Kuhn, (1992), o modelo de controle de acesso baseado em papéis, também denominado *Role Based Access Control*, tornou-se predominante, e aplicações que o utilizam podem ser encontradas nas mais diversas áreas, desde a medicina (EVERED; BÖGEHOLZ, 2004) até a área militar (FERNANDEZ, 2005). Isso porque o modelo CABP não apenas reduz a complexidade de gerenciamento, mas também reduz o

custo administrativo em ambientes com grande freqüência de mudanças.

No modelo CABP, os privilégios de acesso a recursos são associados aos sujeitos de forma indireta, através da utilização de papéis. Esses papéis que, em analogia ao ambiente corporativo, podem ser considerados como as funções de um determinado indivíduo, permitem que a estrutura organizacional de uma organização seja mapeada para dentro do modelo de controle de acesso. Dessa forma, é possível aderir aos objetivos de uma organização sem que haja inferência nas responsabilidades dos indivíduos.

Associar privilégios de forma indireta implica em algumas vantagens quando o CABP é comparado a outros modelos de controle de acesso. Essa característica, por estar em alinhamento com o dinamismo das organizações, faz com que seja possível delegar ou mesmo transferir privilégios a outras entidades através de uma pequena quantidade de tarefas administrativas. Outras vantagens inerentes ao CABP, como, por exemplo, a segregação de poderes, ou mesmo o gerenciamento centralizado, também devem ser levados em consideração, uma vez que proporcionam maior controle das concessões de acesso.

3.2. DISTRIBUIÇÃO DE CREDENCIAIS

Para que os modelos de controle de acesso CABP, CAD e até mesmo CAM sejam utilizados de forma eficaz, é preciso que os mecanismos de execução tenham em mãos informações relacionadas às entidades finais. Essas informações, por expressarem uma qualificação, uma característica que determinada entidade possui, são denominadas credenciais, e podem ser representadas, por exemplo, através das associações de um usuário a determinados grupos. Dessa forma, o mecanismo de execução assume o papel de verificador de privilégios que, antes de tomar qualquer decisão de acesso, tem a responsabilidade de

examinar a veracidade e a validade dessas informações. Observa-se que, aqui, a maneira através da qual se faz a identificação da entidade final é irrelevante. Assume-se que, durante os processos de controle de acesso, como pode ser observado na Figura 4, a autenticação foi realizada de forma bem-sucedida.

O armazenamento e a distribuição de credenciais podem acontecer de diversas maneiras, desde bancos de dados até certificados digitais. Para auxiliar no processo de distribuição, dois modelos fundamentais podem ser considerados: o modelo de apresentação, também conhecido como *push*, e o modelo de obtenção de credenciais, ou *pull*.

3.2.1. O modelo de apresentação

Em algumas situações, pode haver a necessidade de que a entidade final apresente ao verificador de privilégios todas as credenciais necessárias para que as decisões de concessão de acesso possam ser tomadas. Com isso, o verificador de privilégios está isento das responsabilidades de obtenção de tais informações. Não é preciso consultar fontes externas. Esse modelo, ilustrado na Figura 5, melhora o desempenho do sistema ao qual se aplica, uma vez que a carga de trabalho assinalada ao verificador de privilégios é reduzida. Além disso, a entidade final tem a possibilidade de apresentar apenas as credenciais que deseja.

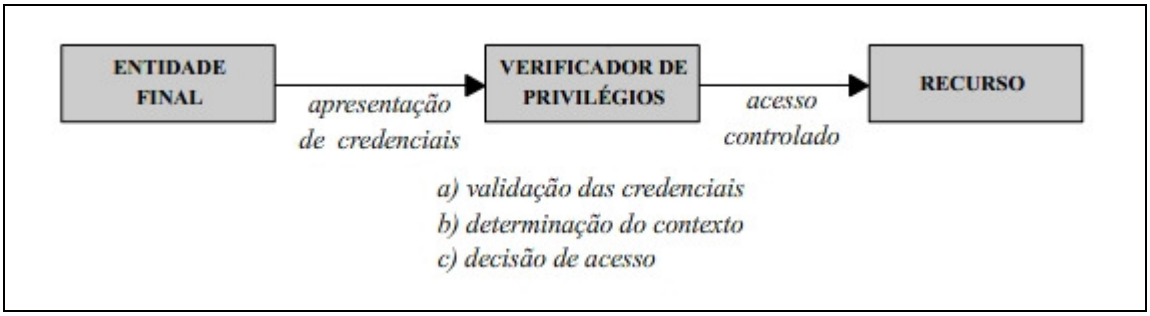

Figura 5. Modelo de apresentação de credenciais.

3.2.2. O modelo de obtenção

Em outros casos, é interessante que a obtenção de credenciais fique sob responsabilidade do verificador de privilégios, que deve comunicar-se, de alguma forma, com entidade externas. Ao consultar entidades tais como uma base de dados, o verificador de privilégios recebe uma carga extra de trabalho, já que ele, além de validar a identidade da entidade final, deve comunicar-se com entidades externas para obter as credenciais necessárias. Esse modelo, conhecido como modelo *pull*, é ilustrado na Figura 6.

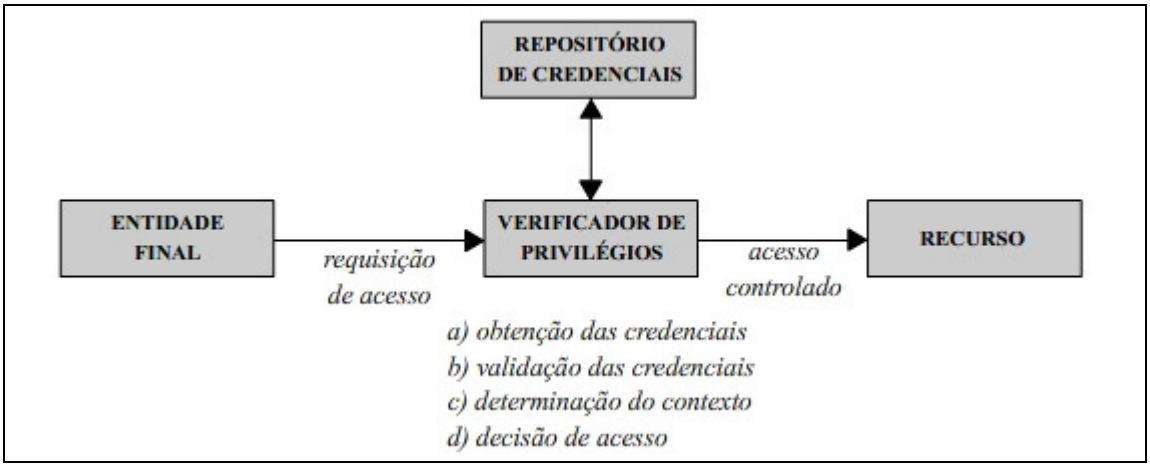

Figura 6. Modelo de obtenção de credenciais.

3.2.3. Comparação entre os modelos

A discussão sobre qual abordagem de distribuição de credenciais deve ser adotada em um sistema que utilize certificados digitais é ampla. Crampton e Khambhammettu (2003) e Seitz, Pierson e Brunie (2005) apresentam em seus trabalhos pontos de vista diferentes, resumidos a seguir:

- Segundo Crampton e Khambhammettu (2003), o modelo de obtenção de credenciais, mesmo degradando o desempenho do sistema ao qual se aplica, ainda é a melhor abordagem a ser considerada. Isso porque o modelo de apresentação, mesmo isentando o verificador de privilégios das responsabilidades de obtenção de credenciais, exige que este realize operações para checar a veracidade e a validade das informações apresentadas.

- Seitz, Pierson e Brunie (2005) afirmam que o modelo de obtenção de credenciais, além de sobrecarregar o verificador de privilégios não permite que as asserções realizadas durante as decisões de controle de acesso sejam temporariamente separadas de uma requisição. Isso significa que, sempre que uma requisição for feita para um mesmo recurso, as regras aplicadas serão as mesmas.

- A abordagem de apresentação de credenciais, na qual o requisitante provê todas as informações necessárias, é a mais apropriada para lidar com permissões em ambientes com grande freqüência de mudanças (SEITZ; PIERSON; BRUNIE, 2005).

- Ainda de acordo com Seitz, Pierson e Brunie (2005), para o modelo de obtenção de credenciais, visto que o verificador de privilégios obtém por si só toda a informação de autorização necessária, aplicar o princípio do menor privilégio para cada operação torna-se uma atividade quase impossível para as entidades finais. Sem que estas percebam, verificadores de privilégios mal configurados ou mal-intencionados podem obter mais informações de autorização do que o necessário[4].

---

[4] O trabalho Shibboleth (CANTOR; ERDOS, 2005) propõe uma solução para o problema de utilização das informações de autorização que envolve políticas de liberação de permissões. Com isso, à entidade final é

Por exemplo: caso uma determinada entidade esteja associada tanto a um grupo de usuários comuns quanto a um grupo de administradores, o privilégio considerado durante o acesso a um recurso será sempre o mesmo. Não é dada à entidade final a chance de escolher qual privilégio deve ser utilizado. Mesmo assim, Burruss (2005) afirma que, do ponto de vista da entidade final, a apresentação de credenciais pode complicar o acesso a recursos, devido à responsabilidade sobre o gerenciamento das credenciais que é passada à entidade final.

- No modelo de obtenção de credenciais, segundo Crampton e Khambhammettu (2003), não é necessário realizar modificações no lado da entidade final. Em outras palavras, a forma com a qual a comunicação entre entidade final e verificador de privilégios toma parte permanece inalterada.

Outros autores, a exemplo de Nochta, Ebinger e Abeck (2002), ressaltam que o modelo de obtenção de credenciais cria uma grande dependência da infra-estrutura existente. A menos que existam meios de armazenamento temporário das credenciais, o que, por sua vez, pode levar aos eventuais problemas de sincronismo, o verificador de privilégios tem suas decisões fortemente ligadas à disponibilidade da infra-estrutura.

---

proporcionado um meio de restringir, através de opções de configuração, os privilégios que devem ser considerados em uma requisição. Entretanto, Seitz, Pierson e Brunie (2005) avaliam essa abordagem como mais dispendiosa e menos intuitiva do que simplesmente selecionar a permissão a ser utilizada.

3.3. O ARCABOUÇO X.812

Com o intuito de promover a padronização, a recomendação X.812 (ITU-T, 1995) definiu um arcabouço geral de controle de acesso, ilustrado na Figura 7. Utilizado como ponto de partida em diversos projetos, inclusive o trabalho relacionado PERMIS (CHADWICK; OTENKO, 2002a), o arcabouço X.812 tem por objetivo demonstrar como os conceitos relacionados ao controle de acesso podem ser especializados para suportar serviços e mecanismos de controle de acesso já difundidos. Outros objetivos podem ser citados, entre eles a identificação dos requisitos de gerenciamento necessários para suportar as operações de concessão de acesso, ou, ainda, a interação entre serviços e mecanismos.

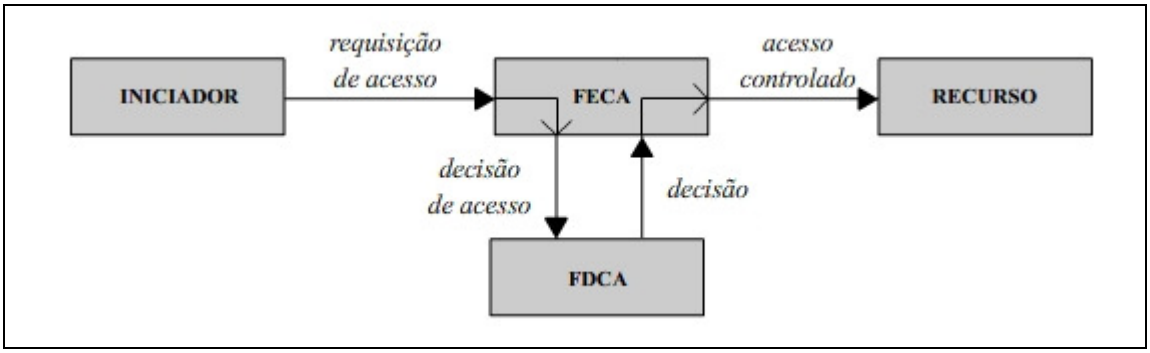

Figura 7. Arcabouço X.812, adaptado de ITU-T (1995).

Conforme as definições do arcabouço X.812, em uma requisição de acesso, quatro elementos devem estar presentes[5]. Além do iniciador da requisição e do próprio recurso a ser acessado, tem-se as funções de execução e de decisão. A primeira dessas funções, denominada Função de Execução do Controle de Acesso (FECA), ou *Access Control*

[5] Observa-se que esse trabalho não adota a nomenclatura original para os elementos formadores do arcabouço X.812 (ITU-T, 1995). Há uma adaptação para a língua portuguesa.

Enforcement Function, é responsável por mediar todas as requisições de acesso. Sempre que necessário, a FECA deve agrupar todas as informações do iniciador e do recurso que sejam relevantes para a determinação do contexto da requisição de acesso. Essas informações, denominadas Informações de Controle de Acesso (ICA), ou *Access Control Information*, fazem com que seja possível interagir, geralmente através de interfaces de programação de autorização, com a Função de Decisão de Controle de Acesso (FDCA), ou *Access Control Decision Function*. A Figura 8 ilustra os relacionamentos entre os elementos formadores do arcabouço X.812.

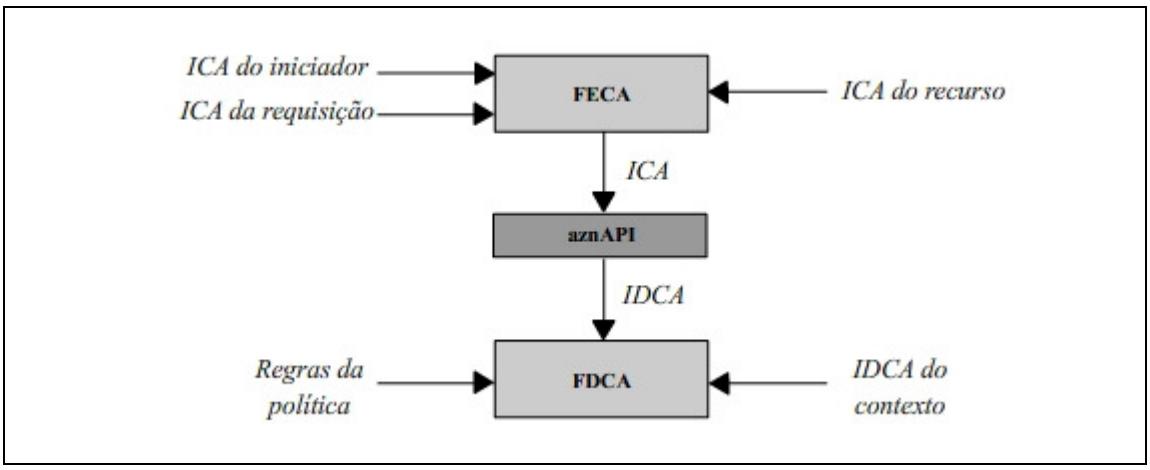

Figura 8. Interação entre os elementos do arcabouço X.812, adaptado de ITU-T (1995).

A interface de programação *aznAPI* transforma as ICA em um conjunto de informações que pode ser interpretado pela FDCA. Denominado Informação de Decisão para o Controle de Acesso (IDCA), ou *Access Control Decision Information*, esse conjunto é combinado a uma série de informações. Entre elas, há as regras da política de controle de acesso adotada e as informações relacionadas ao contexto do ambiente, tais como o momento da requisição ou mesmo a localização (endereço) da qual a requisição partiu. Assim, a FDCA, ciente de todo o contexto da requisição, pode decidir se deve ou não conceder acesso a um recurso em particular.

Por se tratar de um arcabouço de autorização, assim como o apresentado por

Vollbrecht et al (2000), a recomendação X.812 nada menciona em relação à identificação das entidades finais. Assume-se que, previamente ao processo de autorização, as entidades envolvidas já tenham passado por um processo de autenticação (VOLLBRECHT et al, 2000). Da mesma forma, outros serviços de segurança, tais como a auditoria, também são deixados de lado.

4. A INFRA-ESTRUTURA DE GERENCIAMENTO DE PRIVILÉGIOS

Mesmo diante do exposto na seção 3.2, muitos sistemas fundamentam suas decisões de controle de acesso apenas em certificados de chave pública. Em algumas circunstâncias, isso é suficiente. Entretanto, aplicações no âmbito governamental, corporativo e, principalmente, na área médica, têm mostrado que isso não é suficiente. O controle baseado em regras e papéis é necessário (ARSENAULT; TURNER, 2002). Esse tipo de decisão de controle de acesso requer informações adicionais normalmente não incluídas em um certificado de chave pública. Para suportar esse requerimento, e, por conseqüência, promover a separação entre informações de autenticação e autorização, surgiu o Certificado de Atributos (CA), ou *Attribute Certificate*.

De acordo com Shirey (2000), um certificado de atributos é um certificado digital que associa, de forma direta ou indireta, um conjunto de informações a uma entidade final. A associação indireta faz com que um CA se relacione logicamente a um CCP. Na verdade, um certificado de atributos é muito similar a um certificado de chave pública. A principal diferença é que através de um CA não são estabelecidas garantias acerca da autenticidade do proprietário. Em outras palavras, um CA não contém uma chave pública. Ao invés disso, ele contém atributos que determinam associações a grupos, papéis, privilégios de segurança ou qualquer outra informação associada ao proprietário do certificado.

A fim de esclarecer o conceito de certificado de atributos será utilizada a comparação feita por Farrell e Housley (2002). Nela, um certificado de chave pública deve ser considerado como um passaporte, identificando seu proprietário e com tendências a durar por longos

períodos de tempo. Já um certificado de atributos deve ser considerado como um visto, emitido por uma autoridade diferente e com tempo de vida inferior.

Apesar de ambos os certificados estarem logicamente ligados, seu gerenciamento pode ser feito através de infra-estruturas independentes (DAWSON et al, 2002). Sendo assim, de forma semelhante à ICP, a criação dos certificados de atributos deu origem à necessidade por procedimentos que possibilitassem um gerenciamento de certificados eficaz. Essa necessidade implicou na criação de um conjunto de políticas e procedimentos necessários para gerenciar, armazenar, distribuir e revogar certificados. Ao adicionar a este conjunto componentes de hardware e software, bem como o elemento humano, surgiu a Infra-estrutura de Gerenciamento de Privilégios (IGP).

4.1. COMPONENTES

Da mesma forma observada na ICP, a IGP, além de definir a estrutura das informações armazenadas pelos certificados, define as entidades e o papel que cada uma delas deve exercer[6]. Seus componentes, baseados nas descrições encontradas nos trabalhos de Farrell e Housley (2002) e Chang-Ji, Jian-Ping e Hai-Xin (2003) são ilustrados na Figura 9. De acordo com Farrell e Housley (2002), essa ilustração representa uma visão abstrata dos relacionamentos entre as entidades envolvidas na troca de certificados de atributos.

---

[6] Observa-se que esse trabalho não adota a nomenclatura original para os elementos pertencentes à IGP nem mesmo para os campos pertencentes ao certificado de atributos. A nomenclatura original, encontrada na recomendação X.509 (ITU-T, 2000), é adaptada para a língua portuguesa.

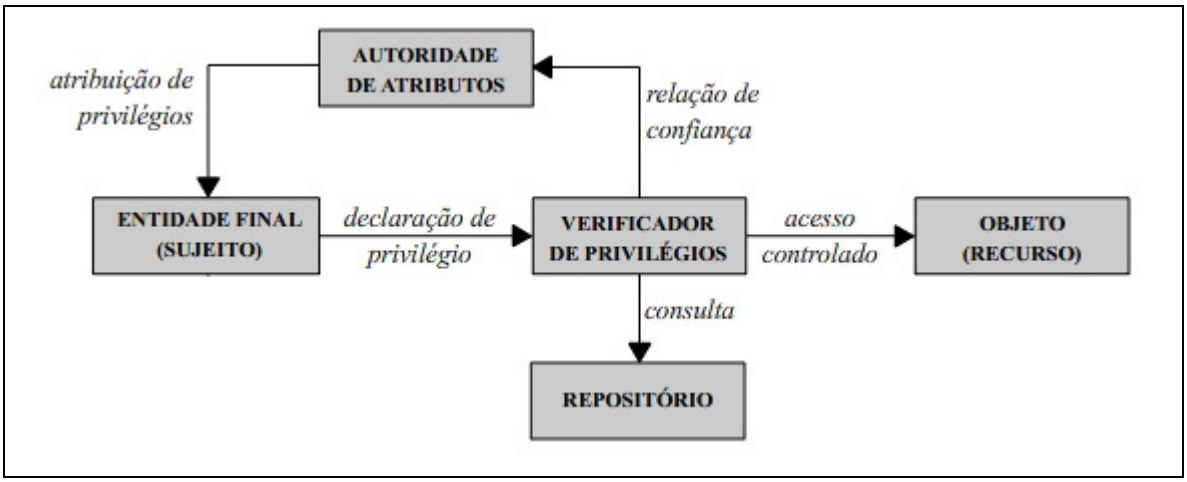

Figura 9. Modelo arquitetural de uma IGP, adaptado de Farrell e Housley (2002).

Os componentes de uma IGP são os seguintes:

- **Entidade Final**. Também conhecido pelo termo sujeito, ou mesmo proprietário, esse componente representa os usuários finais, ou seja, qualquer entidade que possuir um certificado de atributos;
- **Autoridade de Atributos (AA)**. Esse componente, em analogia com a ICP, pode ser considerado como uma AC, visto que a emissão, o gerenciamento e a revogação de certificados digitais também são de sua responsabilidade. A diferença é que a AA lida apenas com certificados de atributos. Em relação à revogação, é importante ressaltar que, na IGP, esse processo pode ou não ser necessário. Em alguns ambientes, o certificado de atributos pode possuir períodos de validade muito curtos, fazendo com que a necessidade de revogação seja inexistente. Mas, se por alguma razão, uma autoridade revogar um certificado de atributos previamente emitido, as entidades precisam, de alguma forma, estar aptas a aprender que a revogação ocorreu para que não se utilize um certificado não confiável. Para isso, há outro elemento sob sua responsabilidade: a Lista de Certificados de Atributos Revogados (LCAR);

- **Fonte de Autoridade (FA)**. Também conhecido como *Source of Authority*, este termo também é utilizado para representar um AA. A diferença é que a FA só é utilizada caso exista, dentro da arquitetura da IGP, uma hierarquia de Autoridades de Atributos. Caso isso aconteça, a AA raiz é denominada FA;
- **Verificador de Privilégios**. Algumas vezes representado pelo próprio recurso a ser acessado, esse componente é o responsável por validar se as informações contidas no certificado de atributos apresentado pela entidade final são suficientes para atender aos requisitos de segurança existentes;
- **Objeto**. Esse componente representa o recurso a ser controlado e possui métodos de acesso bem definidos, cada qual com um grau de sensibilidade respectivo. Essas e outras informações, tais como varáveis relacionadas ao momento em que as requisições de acesso se iniciaram, são utilizadas pelo verificador para determinar o contexto de acesso;
- **Repositório**. Da mesma forma vista na ICP, o repositório é definido como um meio de armazenamento e distribuição centralizado de certificados e listas de certificados revogados.

4.2. CERTIFICADO DE ATRIBUTOS

Conforme visto anteriormente, um certificado de atributos é muito similar a um certificado de chave pública. As diferenças se concentram, principalmente, nas finalidades para as quais ambos estão designados. Um CCP pode ser utilizado para fins de autenticação, fornecendo garantias acerca da identidade de seu proprietário. Para isso, sua estrutura

armazena informações relacionadas às primitivas da criptografia assimétrica, representadas pela chave pública (vide o Apêndice A). Já um AC, por não possuir esse propósito, não precisa comportar tais informações.

Certificados de atributos devem ser utilizados para alcançar objetivos associados ao controle de acesso, à autenticação da origem da informação e ao não-repúdio (ITU-T, 2000). Em relação ao controle de acesso, os atributos contidos no CA são utilizados para expressar associações a grupos ou privilégios que as entidades finais possuam. Com isso, os elementos responsáveis pelas decisões de concessão de acesso devem se assegurar de que o proprietário do CA é realmente a entidade requisitante. Quanto à autenticação da origem da informação e ao não-repúdio, os atributos contidos em um CA são utilizados para prover informações adicionais sobre a entidade final, podendo ser utilizados para assegurar que a entidade está autorizada a realizar assinaturas.

Para satisfazer a essas condições, a estrutura do CA, representada na Figura 10, deve suportar algum mecanismo de referência a certificados de chave pública. Através desse mecanismo é possível promover a utilização conjunta de serviços de autenticação e autorização, aumentando o grau de segurança proporcionado a sistemas que utilizam certificados digitais.

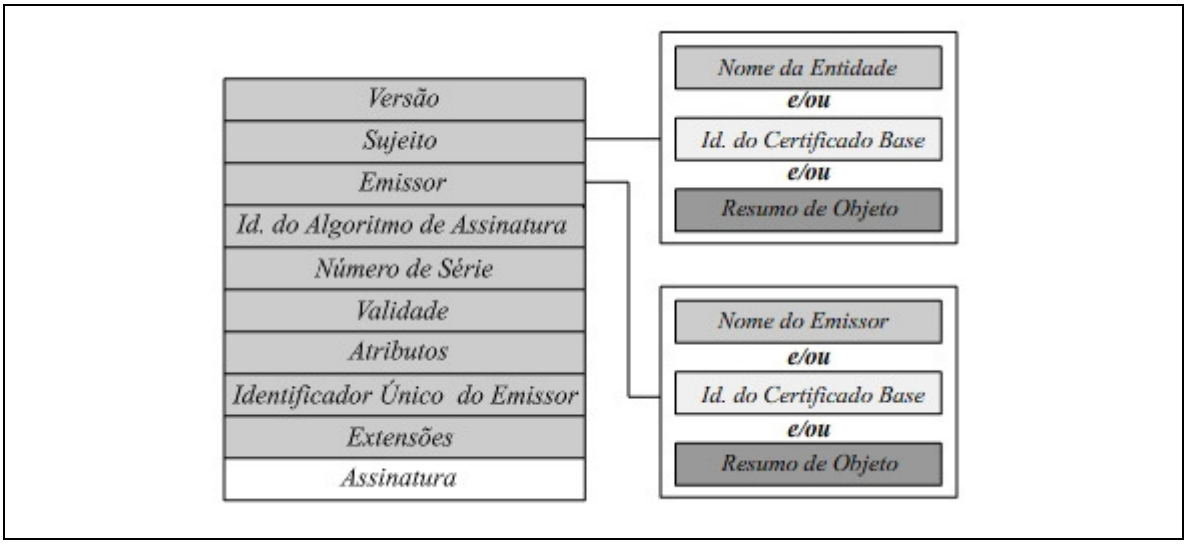

Figura 10. Estrutura do Certificado de Atributos X.509.

Os campos existentes na estrutura do CA são os seguintes:

- `Versão`. Identifica a versão do formato do certificado de atributos;
- `Sujeito`. Representa a identidade do proprietário do certificado ou o papel ao qual a entidade final está relacionada. Esse campo pode ser formado pelo conjunto de uma ou mais das seguintes informações: (1) `Nome da Entidade`, que indica o nome da entidade final ou papel ao qual ela está associada; (2) `Identificação do Certificado Base`, que indica o número de série do certificado de chave pública da entidade final e o nome do emissor do respectivo CA; e (3) `Informações sobre Resumo de Objeto`, que contém um resumo criptográfico (ver Apêndice A) de qualquer objeto que possa ser utilizado para identificar e/ou autenticar uma entidade final. Se o componente (1) for o único presente, qualquer certificado de chave pública que possuir um desses nomes pode ser usado para autenticar a identidade do proprietário. Se, além de (1), o componente (2) também

estiver presente, apenas o certificado especificado por este último deve ser utilizado[7]. Já o componente (3), se presente, é usado diretamente para identificar ou autenticar a identidade do proprietário, sem que a localização de um certificado de chave pública seja necessária;

- `Emissor`. O campo emissor representa a entidade emissora do certificado (AA) e, da mesma forma observada no campo Sujeito, pode ser formado pelo conjunto de uma ou mais das seguintes informações: (1) `Nome do Emissor`, (2) `Identificação do Certificado Base` e (3) `Informações sobre Resumo de Objeto`;

- `Identificador do Algoritmo de Assinatura`. Identifica o algoritmo criptográfico utilizado no momento da geração da assinatura digital contida no certificado;

- `Número de Série`. Campo responsável por identificar o certificado de forma única dentro do escopo do emissor;

- `Validade`. Define o intervalo de tempo durante o qual o certificado de atributos deve ser considerado válido;

- `Atributos`. Campo que contém os atributos (privilégios) associados com o proprietário que está sendo certificado;

- `Identificador Único do Emissor`. Pode ser utilizado para identificar o emissor do certificado em casos em que o conteúdo do campo `Emissor` não for

[7] Em casos como esse, o campo `Nome da Entidade` serve apenas como ferramenta de auxílio para que o verificador de privilégios possa localizar o certificado de chave pública correspondente (ITU-T, 2000).

suficiente;

- `Extensões`. Da mesma forma observada para certificados de chave pública, o campo extensões permite que novos campos sejam adicionados à estrutura original.

4.2.1. Questões relacionadas à identificação

ITU-T (2000) ressalta que, devido ao fato de os campos `Sujeito` e `Emissor` serem formados inteiramente por elementos opcionais, há riscos em se utilizar apenas as opções `Nome da Entidade` e `Nome do Emissor` para que se identifiquem, respectivamente, o proprietário e emissor do certificado de atributos. Visto que esse tipo de informação é geralmente insuficiente para que se identifique uma entidade de forma adequada, uma combinação de elementos, assim como sugerido na recomendação X.509, poderia ser utilizada para solucionar essa questão. No entanto, Farrell e Housley (2002) recomendam que uma única opção, preferencialmente o Identificador do Certificado Base, seja utilizada.

O campo `Identificador do Certificado Base` combina algumas das informações contidas no certificado de chave pública pertencente à entidade final, como, por exemplo, o número de série e o nome do emissor. Dessa forma, utilizar esse campo para identificar a entidade final faz com que o emissor do certificado de atributos confie nos processos de autenticação realizados pela AC. Entretanto, a autenticação da entidade final, ao invés de estar diretamente relacionada a um CCP, pode acontecer de forma independente. Utilizando o campo `Informações sobre Resumo de Objeto`, é possível armazenar-se o resumo criptográfico (vide Apêndice A) de qualquer objeto. Esse resumo, durante o processo de autenticação, é então comparado com um resumo enviado pelo proprietário do certificado

de atributos (SOUZA et al, 2004). Caso os dois resumos sejam equivalentes, a autenticidade das informações pode ser verificada, permitindo a identificação da entidade final sem que se estabeleçam vínculos diretos entre o CA e o CCP.

4.3. MODELOS

São definidos na recomendação X.509 (ITU-T, 2000) quatro modelos de funcionamento para a IGP: o modelo geral, o de controle, o de delegação e o de papéis. Cada qual possui características peculiares, abordadas nas subseções a seguir.

4.3.1. Modelo Geral

O modelo geral de gerenciamento de privilégios, representado na Figura 11, pode ser considerado, segundo Souza et al (2004), como o mais genérico, visto que serve de base para a maioria das infra-estruturas IGP existentes. Conforme observado em ITU-T (2000), há, nesse modelo, três entidades: o objeto, o sujeito e o verificador de privilégios. O objeto representa o recurso sendo protegido; o sujeito representa a entidade à qual são atribuídos os privilégios de acesso; o verificador de privilégios, por sua vez, é a entidade responsável por determinar se, em um determinado contexto, os privilégios atribuídos aos sujeitos são suficientes para que o acesso ao objeto possa tomar parte. Essa determinação depende de, no mínimo, quatro fatores (ITU-T, 2000): os privilégios do sujeito, a política de segurança em questão, as variáveis de ambiente e as características do objeto.

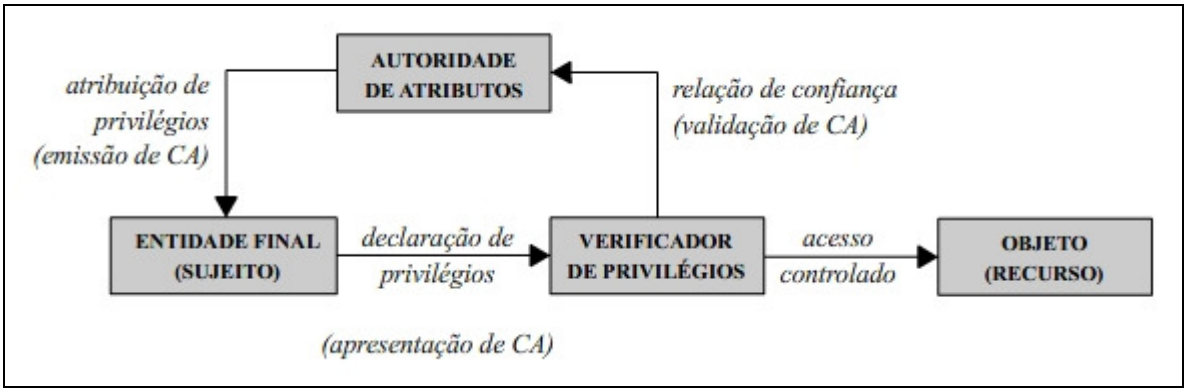

Figura 11. Modelo geral da IGP.

A Autoridade de Atributos (AA) é a responsável por atribuir privilégios ao sujeito. Esse conjunto de privilégios representa uma associação entre entidade final e atributos de autorização. Sempre que uma requisição de acesso ao objeto tomar parte, a validade dessa associação é examinada pelo verificador de privilégios, que também deve levar em consideração informações relacionadas ao contexto de acesso, tais como o momento da requisição, a sensibilidade do objeto sendo acessado, ou mesmo a política de segurança.

A política de segurança, que precisa ser protegida para os quesitos de integridade e autenticidade, especifica o grau de privilégios considerado suficiente para que se efetue o acesso ao recurso. Com ela, o verificador de privilégios determina, para um dado conjunto de informações, o limite de aceitação mínimo para que o acesso possa tomar parte. Na recomendação X.509 não há definição de qual sintaxe deve ser utilizada para expressar uma política. Dessa forma, segundo Chadwick, Otenko e Ball (2003), uma das tarefas mais significantes do trabalho relacionado PERMIS é propor uma sintaxe para as políticas de autorização.

4.3.2. Modelo de Controle

O modelo de controle não deve ser considerado como uma das possíveis arquiteturas de funcionamento da IGP, mas sim como uma forma de ilustrar que tipo de informação o verificador de privilégios deve considerar para determinar o contexto da requisição de acesso. O modelo de controle, representado na Figura 12, é formado pelos seguintes componentes: o sujeito, o verificador de privilégios, as características do recurso sendo protegido, a política de privilégios e as varáveis de ambiente.

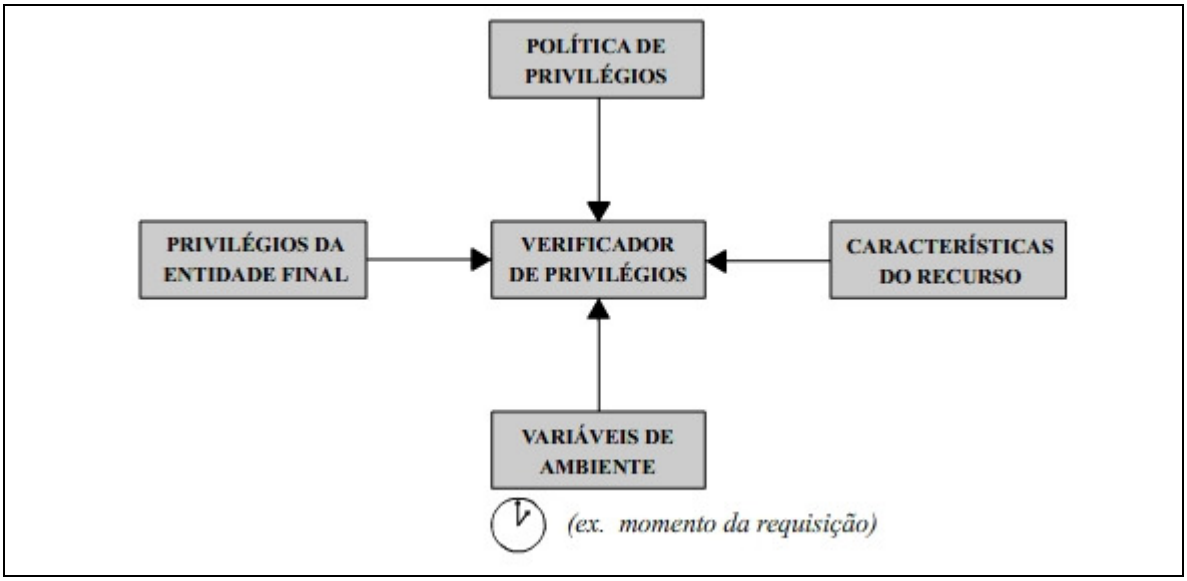

Figura 12. Modelo de controle da IGP, adaptado de ITU-T (2000).

4.3.3. Modelo de Delegação

O modelo de delegação, conforme observado na Figura 13, é formado pelos seguintes componentes: o proprietário do privilégio (representado na figura pela Autoridade de Atributos), o sujeito para o qual o privilégio foi delegado, o verificador de privilégios e a

Fonte de Autoridade.

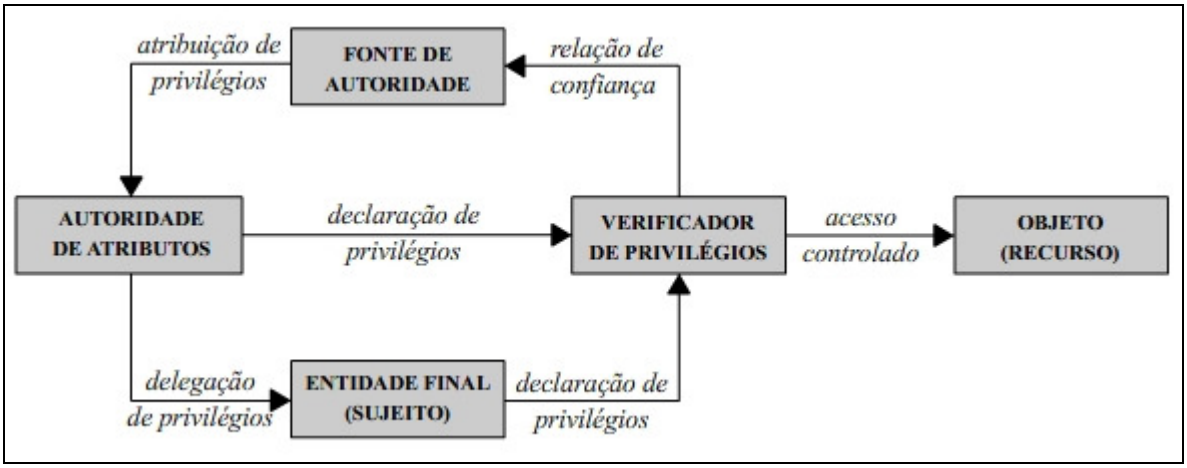

Figura 13. Modelo de delegação da IGP, adaptado de ITU-T (2000).

Algumas vezes, quando houver a necessidade de se delegarem privilégios, seu proprietário deve estar autorizado a associá-los a outras entidades. Em outras palavras, o proprietário de um privilégio que deseja realizar a delegação deve estar capacitado a agir como uma entidade emissora de certificados. Posteriormente, cada uma das entidades para as quais esses privilégios foram delegados também pode, opcionalmente, fazer o mesmo.

Esse encadeamento de privilégios dá origem aos caminhos de delegação (*delegation paths*) que, embora análogos aos caminhos de certificação de uma ICP (KNIGHT; GRANDY, 2002), são considerados distintos (ITU-T, 2000). Todavia, o mecanismo responsável pela determinação da validade de um caminho de delegação, no curso de suas atividades, deve considerar os elementos associados tanto à IGP quanto à própria ICP. E, para que o modelo de delegação seja eficaz, é preciso que esses caminhos sejam validados por completo.

A fim de evitar cadeias muito extensas, é possível, com o auxílio da extensão `basicAttConstraints`, limitar a habilidade de delegação posterior. A estrutura dessa extensão, representada em sua notação ASN.1 na Figura 14, possui os seguintes campos: `authority`, que pode inibir a delegação por completo, e `pathLenConstraint`, que pode restringir o tamanho da cadeia de delegação.

```
basicAttConstraints EXTENSION ::= {
  SYNTAX BasicAttConstraintsSyntax
  IDENTIFIED BY { id-ce-basicAttConstraints }
}

BasicAttConstraintsSyntax ::= SEQUENCE {
  authority BOOLEAN DEFAULT FALSE,
  pathLenConstraint INTEGER (0..MAX) OPTIONAL
}
```

Figura 14. Extensão para limitação de delegação posterior.

Além de limitar a delegação posterior, também é possível delegar apenas um conjunto de privilégios. De qualquer forma, independente das restrições que podem ser aplicadas aos privilégios delegados, uma restrição universal do modelo de delegação é que nenhuma entidade pode delegar mais privilégios do que possui (ITU-T, 2000).

4.3.4. Modelo Baseado em Papéis

Papéis proporcionam meios para que privilégios sejam associados a indivíduos de forma indireta. Em ambientes distribuídos e com grande freqüência de mudanças, essa característica torna o gerenciamento mais simples, já que para atribuir um conjunto de privilégios a uma entidade basta associá-la a um determinado grupo. Além disso, através do modelo baseado em papéis, assim como observado na subseção 3.1.3, a estrutura organizacional de uma companhia pode ser mapeada para dentro do modelo de controle de acesso sem que haja inferência na responsabilidade dos indivíduos.

Outro fator positivo a ser considerado é que o modelo baseado em papéis permite que os privilégios associados a um determinado papel sejam gerenciados sem que qualquer impacto recaia sobre o relacionamento entre papel e entidade. Para isso, no modelo de gerenciamento de privilégios baseado em papéis, ao menos dois tipos de certificados de

atributos devem existir: o Certificado de Especificação de Papel (CEP) e o Certificado de Relacionamento a Papéis (CRP).

O Certificado de Especificação de Papel é responsável por associar um conjunto de privilégios a um determinado papel e deve, exclusivamente, ser expresso sob a forma de um CA. Já o Certificado de Relacionamento a Papéis, responsável por associar a entidade final a um papel, pode ser expresso tanto sob a forma de um CA quanto de um CCP (vide subseção 2.3). A afiliação a um papel, assim como qualquer outro privilégio, pode ser delegada a outras entidades, dando origem a um modelo de gerenciamento que, além das características relacionadas ao modelo baseado em papéis, engloba características do modelo de delegação.

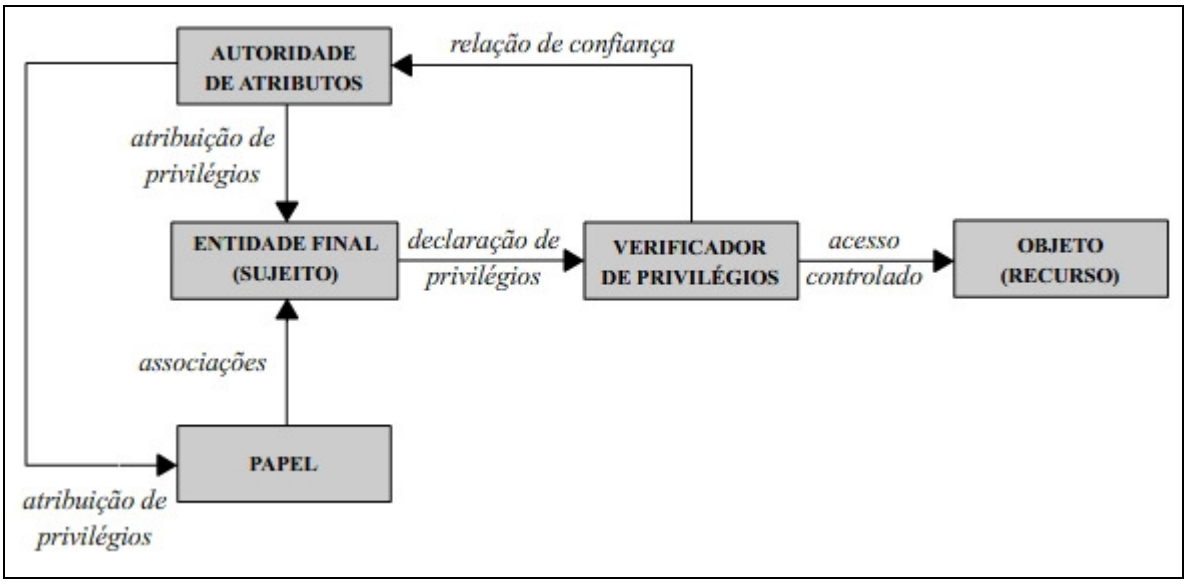

Figura 15. Modelo baseado em papéis da IGP.

Conforme observado na Figura 15, durante uma requisição de acesso a um recurso, o sujeito apresenta seu certificado de relacionamento ao verificador de privilégios que, por sua vez, deve determinar quais são os privilégios associados àquele papel. Assim, o verificador de privilégios deve ter à sua disposição os certificados de especificação de papel antes de tomar as decisões relacionadas à concessão de acesso.

4.3.4.1. Relacionamento entre certificados

Para que autorização e conseqüente controle de acesso aconteçam conforme as características do CABP, é preciso que os certificados CRP e CEP mantenham algum tipo de vínculo. Esse relacionamento entre certificados é feito com o auxílio da extensão identificadora `roleSpecCertIdentifier`, representada na Figura 16 em sua notação ASN.1.

```
roleSpecCertIdentifier EXTENSION ::= {
    SYNTAX RoleSpecCertIdentifierSyntax
    IDENTIFIED BY { id-ce-roleSpecCertIdentifier }
}

RoleSpecCertIdentifierSyntax ::= SEQUENCE SIZE
    (1..MAX) OF RoleSpecCertIdentifier

RoleSpecCertIdentifier ::= SEQUENCE {
    roleName             [0] GeneralName,
    roleCertIssuer       [1] GeneralName,
    roleCertSerialNumber [2] CertificateSerialNumber OPTIONAL,
    roleCertLocator      [3] GeneralNames OPTIONAL
}
```

Figura 16. Extensão identificadora de certificado de especificação de papel.

Através dessa extensão, um mesmo CRP pode relacionar-se a múltiplos CEPs de uma única vez. Dessa forma, sua estrutura é composta por uma ou mais instâncias do elemento `RoleSpecCertIdentifier` que, por sua vez, armazena os seguintes elementos:

- `roleName`, que especifica o nome do papel em questão, fazendo referência ao campo `Sujeito` do CEP;
- `roleCertIssuer`, que indica o nome do emissor do CEP;
- `roleCertSerialNumber`, que indica o número de série do CEP;
- `roleCertLocator`, que armazena informações adicionais sobre o CEP.

4.4. RELAÇÕES COM A INFRA-ESTRUTURA ICP

A IGP é análoga à ICP no tocante à responsabilidade de cada um de seus elementos formadores (CHADWICK; OTENKO, 2002a). Contudo, as autoridades emissoras de certificados dessas infra-estruturas são logicamente e, em muitas vezes, fisicamente independentes (ITU-T, 2000). Dessa forma, as funcionalidades de criação e de manutenção de uma identidade podem, e quase sempre devem, estar separadas da IGP.

No entanto, para que as decisões de concessão de acesso possam acontecer, é preciso, entre outras coisas, que se identifique a entidade que iniciou uma requisição. Atender a essa necessidade se faz possível através das práticas de autenticação oferecidas pela ICP. Logo, para que se estabeleça uma IGP, é pré-requisito que exista uma ICP em total operação.

CONCEITO	ENTIDADE ICP	ENTIDADE IGP
Certificado	*Certificado de Chave Pública (CCP)*	*Certificado de Atributos (CA)*
Emissor de Certificados	*Autoridade Certificadora (AC)*	*Autoridade em Atributos (AA)*
Emissor Raiz	*Autoridade Certificadora Raiz*	*Fonte em Autoridade (FA)*
Revogação	*Lista de Certificados Revogados (LCR)*	*Lista de Certificados de Atributos Revogados (LCAR)*

Figura 17. ICP x IGP: relações entre as entidades.

Conforme observado na Figura 17, as entidades de ambas as infra-estruturas possuem responsabilidades muito similares. Por exemplo: a AC raiz é a entidade na qual se tem máxima confiança para os procedimentos de validação de uma identidade. Já a FA é a entidade na qual o verificador de privilégios confia como a máxima autoridade responsável pela atribuição de privilégios.

4.5. AQUISIÇÃO DE PRIVILÉGIOS

Uma entidade pode adquirir privilégios sem executar uma ação sequer, ou até mesmo sem ter o conhecimento explícito das atividades de associação que tomaram parte (ITU-T, 2000). Um privilégio é dado à entidade por iniciativa própria da AA ou por solicitação de uma terceira entidade. Geralmente, em esquemas com essa característica, o certificado de atributos criado é armazenado em um repositório de acesso público. Dessa forma, a cada requisição, a fim de determinar o contexto de acesso, o verificador de privilégios deve seguir o modelo de obtenção de credenciais visto na subseção 3.2.2.

De forma alternativa, uma entidade pode requisitar um privilégio a uma AA. Uma vez criada, essa associação, sob a forma do certificado de atributos, pode ser retornada apenas à entidade requisitante, sem estar disponível ao acesso público. Com isso, a cada requisição a um recurso protegido, a entidade final deve prover o certificado de atributos ao verificador de privilégios, conforme o modelo de apresentação de credenciais observado na subseção 3.2.1.

Em ambos os procedimentos de aquisição de privilégios anteriormente descritos, é preciso que a AA se assegure de que a entidade realmente deve se relacionar àquele privilégio. Isso pode envolver mecanismos de registro análogos aos procedimentos de certificação realizados na ICP durante a criação de identidades.

5. ESTUDO DE CASO: PERMIS

A utilização de certificados digitais para controle de acesso a recursos pode ser observada em trabalhos de autores como Johnston, Mudumbai e Thompson (1998) e Erdos e Cantor (2005). No entanto, apenas um trabalho, por se utilizar amplamente de alguns dos padrões existentes, serve de base para o modelo proposto nessa dissertação, e será discutido aqui: o PERMIS (CHADWICK; OTENKO, 2002a).

O PERMIS, um projeto fundando pela Comissão Européia, tem o objetivo de construir uma IGP baseada nos certificados de atributos X.509 que utilize o modelo de controle de acesso baseado em papéis, CABP (vide seção 3.1.3). Atualmente presente em sistemas das cidades européias de Bolonha, Barcelona e Salford, o PERMIS pode ser utilizado como alternativa para suporte a funcionalidades de autorização em uma grande variedade de áreas, inclusive a área médica. Uma de suas principais características é o fato de ser agnóstico à autenticação, ou seja, a tarefa de identificar as entidades é deixada a cargo das aplicações que, com isso, podem escolher que tipo de mecanismo utilizar.

Em relação ao método de distribuição de credenciais, o PERMIS utiliza o modelo de obtenção, no qual todos os certificados envolvidos no processo de autorização, inclusive o certificado que armazena a política, são armazenados em um repositório central de acesso público. Como resultado, a utilização de listas de revogação de certificados não é mais necessária, uma vez que a AA pode simplesmente remover de seu repositório os certificados que não são mais válidos.

5.1. ARQUITETURA

A arquitetura de funcionamento do PERMIS é composta pelo subsistema de alocação, responsável por atribuir privilégios às entidades finais, e pelo subsistema de verificação, responsável por autenticar e autorizar as entidades. A autenticação é realizada de acordo com os requisitos da aplicação, isto é, uma entidade pode ser autenticada através de diversos mecanismos, desde os mais simples (combinações de usuário e senha), até os mais complexos (chaves assimétricas com certificado digital). Por outro lado, a autorização é independente, ou seja, um único mecanismo de autorização opera, sempre de acordo com a política de autorização adotada, da mesma maneira para todas as aplicações.

5.1.1. A política de autorização

No PERMIS, algumas das informações necessárias para as decisões de autorização são descritas através da linguagem XML por uma política que, para fins de manutenção de integridade, é armazenada em um CA. A escolha da linguagem XML está relacionada, segundo Chadwick, Otenko e Ball (2003), ao fato de que as linguagens existentes não satisfazem por completo os requisitos de funcionamento do PERMIS. Enquanto a linguagem *Ponder* (DAMIANOU et al, 2001), embora compacta e poderosa, possui apenas um pequeno número de ferramentas de suporte, a especificação *KeyNote* (BLAZE; FEIGENBAUM; IOANNIDIS, 1999), ainda que compreensiva, é focada no modelo de controle de acesso discreto, ao invés do CABP (CHADWICK; OTEKNO; BALL, 2003).

A política de autorização do PERMIS é composta pelos seguintes elementos

(CHADWICK; OTENKO, 2002b):

- `SubjectPolicy`, que especifica o domínio de entidades a ser considerado. Apenas as entidades pertencentes a esse domínio podem acessar os recursos protegidos por essa política;
- `RoleHierarchyPolicy`, que determina os papéis e os relacionamentos hierárquicos entre cada um deles;
- `SOAPolicy`, que especifica quais autoridades emissoras podem gerenciar papéis;
- `RoleAssignmentPolicy`, que, além de determinar quais os possíveis relacionamentos entre autoridades emissoras, entidades finais e papéis, também determina o tempo de validade de cada uma dessas associações;
- `TargetPolicy`, que especifica quais são os recursos protegidos pela política;
- `ActionPolicy`, que determina quais são as ações (ou métodos) suportadas pelos recursos devem ser protegidas. Além disso, especifica o conjunto de parâmetros que deve ser passado em conjunto com cada uma dessas ações;
- `TargetAccessPolicy`, que especifica os relacionamentos entre papéis, recursos e ações.

A Figura 18 ilustra apenas um fragmento de uma política de autorização completa, e foi baseada em uma das políticas apresentadas por Chadwick e Otenko (2003).

```
...
<TargetPolicy>
  <TargetDomainSpec ID="impressora">
    <Include LDAPDN="ou=São Paulo, o=Universidade, c=BR"/>
  </TargetDomainSpec>
</TargetPolicy>
...
<ActionPolicy>
  <Action Name="imprimir"/>
</ActionPolicy>
...
<TargetAccessPolicy>
  <TargetAccess>
    <RoleList>
      <Role Type="papel" Value="usuário"/>
    </RoleList>
    <TargetList>
      <Target Actions="imprimir">
        <TargetDomain ID="impressora"/>
      </Target>
    </TargetList>
  </TargetAccess>
</TargetAccessPolicy>
...
```

Figura 18. Exemplo de política de autorização.

Nesse exemplo, a política de autorização especifica que apenas as entidades que possuem associação com o papel “usuário” podem realizar a ação “imprimir” sobre o recurso “impressora”. Além disso, um outro filtro é associado às entidades requisitantes. Apenas as entidades que pertencerem ao domínio especificado por “ou=São Paulo, o=Universidade, c=BR” podem acessar o recurso “impressora”.

5.1.2. O subsistema de alocação de privilégios

O subsistema de alocação de privilégios, ilustrado na Figura 19, é responsável por emitir certificados de associação a papéis para as entidades finais, além de assinar o CA que contém a política de autorização que rege o modelo de controle de acesso. Todos esses certificados são armazenados em um repositório público para uso futuro do verificador de

privilégios.

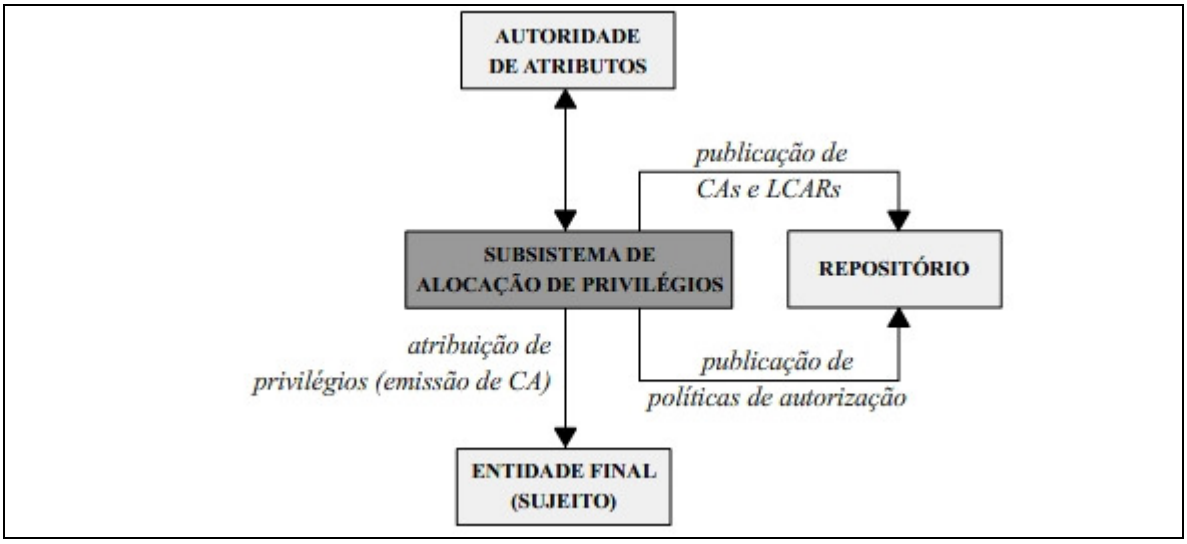

Figura 19. Subsistema de alocação de privilégios.

O repositório, além de armazenar as políticas de autorização, também armazena os certificados de atributos emitidos para as entidades finais. Caso o mecanismo de autenticação escolhido pela aplicação faça uso da ICP, o mesmo repositório pode ser utilizado para armazenar certificados de chave pública e listas de certificados revogados.

5.1.3. O subsistema de verificação de privilégios

Ilustrado na Figura 20, o subsistema de verificação de privilégios é o responsável por autenticar e autorizar as entidades finais (CHADWICK; OTENKO, 2002a). Em concordância com o arcabouço X.812 (vide subseção 3.3), esse subsistema tem suas atividades designadas a dois componentes diferentes: FECA e FDCA.

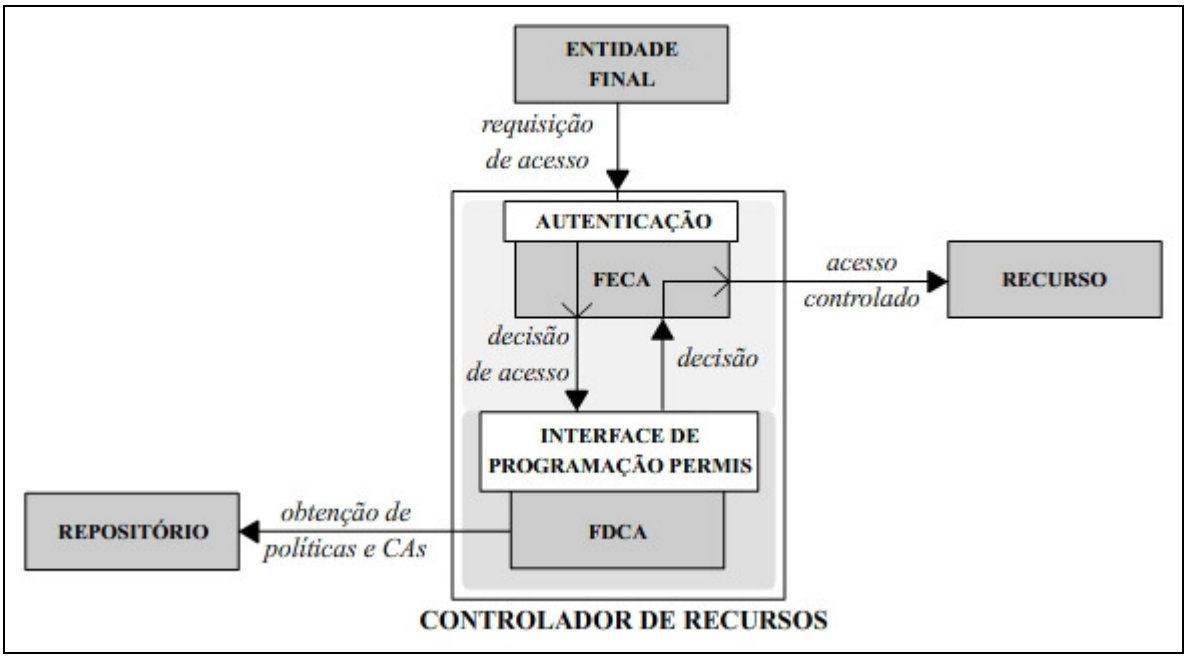

Figura 20. Subsistema de verificação de privilégios, adaptado de Chadwick e Otenko (2002a).

Nesse modelo, durante uma requisição de acesso de acesso, o FECA é responsável por autenticar a entidade final de acordo com as necessidades da aplicação, e verificar, junto à função de decisão (FDCA), se aquela entidade possui privilégios suficientes para realizar uma determinada ação em um recurso em particular. Para isso, a FDCA acessa um ou mais repositórios que contenham as informações necessárias para que se construa o contexto de acesso: políticas de autorização e certificados de atributos da entidade final.

5.2. INTERFACE DE PROGRAMAÇÃO

No PERMIS, a comunicação entre os componentes formadores do subsistema de verificação de privilégios é feita através de uma interface de programação baseada na *aznAPI* (THE OPEN GROUP, 2000). A interface de programação do PERMIS possui as seguintes funções:

- **Iniciar**. Através dessa função, originalmente denominada *Initialise*, a FECA transmite à FDCA as informações que deverão ser consideradas para as decisões de concessão de acesso, dentre elas: o identificador da política de autorização adotada e a localização dos repositórios de onde serão obtidos a política e os certificados de especificação de papéis. Ao término de sua execução, a FDCA terá lido e validado a política de privilégios que irá controlar todas as futuras decisões.

- **ObterCredenciais**. Quando uma entidade inicia uma requisição a um recurso, a FECA é responsável por autenticá-la, utilizando mecanismos específicos da aplicação (combinação de usuário e senha, por exemplo). Em seguida, a FECA é responsável por transmitir à FDCA um descritor capaz de identificar, de forma única, a entidade requisitante. Dessa forma, através da função ObterCredenciais, ou *getCreds*, a FDCA pode obter todos os certificados de atributos associados àquela entidade consultando aos repositórios identificados durante a chamada à função Iniciar. Os certificados obtidos são então analisados e confrontados com os elementos formadores da política de autorização adotada, determinando quais certificados devem ser mantidos e quais devem ser descartados. Observa-se então que o PERMIS utiliza o modelo de obtenção de credenciais descrito no subitem 3.2.2.

- **Decidir**. Após estar devidamente autenticada, a entidade requisitante, no curso de suas atividades, tenta realizar certas operações em um recurso. A cada tentativa, a FECA transmite o nome do recurso, a operação e outros parâmetros para o FDCA através da função Decidir (*Decision*). Ela é responsável por verificar se a ação é permitida para aquela entidade, sempre levando em consideração as condições especificadas na política de privilégios. Se a ação for permitida, a função de decisão retorna ao FECA o valor “Permitido”, do contrário, “Negado”. Cada vez

que uma nova tentativa de conexão se iniciar, uma chamada será feita a essa função, e para evitar que conexões fiquem em espera por uma quantidade de tempo infinita, até mesmo após os certificados expirarem, há no PERMIS o conceito de expiração de sessão.

- **Desligar**. O propósito dessa função, originalmente denominada *Shutdown*, é de terminar a FDCA, fazendo com que as informações por ela armazenadas, inclusive a política em uso, sejam descartadas. Isso pode acontecer em situações em que a AA quer impor dinamicamente uma nova política de autorização para o domínio.

5.3. CONCLUSÃO

Ao analisar as características principais do PERMIS, observa-se que, conforme Meinel e Zhou (2004) e PERMIS (2004), a tarefa de autenticar as entidades é deixada a cargo das aplicações que, com isso, podem escolher que tipo de mecanismo utilizar. Isso pode ser um fator positivo, visto que os mecanismos de autenticação já existentes não precisam ser modificados para suportar a utilização de certificados de chave pública. Em contrapartida, a política de autorização, para identificar os usuários, faz uso de informações presentes apenas nos certificados de chave pública. Com isso, há a necessidade de se manter um esquema de mapeamento entre esse tipo de informação e as informações utilizadas pelos mecanismos de autenticação.

Outras características, como, por exemplo, a delegação de privilégios, também são motivos de análise. No PERMIS, não há mecanismos de suporte à delegação dinâmica de privilégios entre entidades finais. Isso significa que não há meios para que uma entidade final atribua privilégios a outras entidades finais de forma dinâmica sem a anuência de uma terceira

parte.

Além disso, a interface de programação oferecida pelo PERMIS incentiva a construção (ou modificação) das aplicações para que estas façam uso de funcionalidades de autorização.

6. MODELO PROPOSTO

O modelo proposto aqui visa proporcionar a interação entre as infra-estruturas X.509 ICP e IGP para ambientes computacionais que tenham por meta controlar o acesso a aplicações de rede. Utilizando certificados de chave pública e certificados de atributos, esse modelo possibilita que aplicações que lidam com informações sensíveis façam uso, de forma integrada, tanto dos serviços de autenticação quanto dos serviços de autorização oferecidos respectivamente pelas infra-estruturas ICP e IGP.

Quando comparado ao PERMIS[8], o modelo proposto apresenta algumas diferenças que podem ser encontradas, principalmente, nas funcionalidades referentes à autenticação. Enquanto o PERMIS implementa autorização no topo de um sistema de autenticação já existente (PERMIS, 2004), o objetivo do modelo proposto é utilizar os certificados de chave pública X.509 pertencentes à infra-estrutura ICP.

Além disso, outras características, entre elas a interface de programação oferecida pelo PERMIS às aplicações, também são motivos de análise. Neste trabalho, o objetivo, ao invés de incentivar a construção (ou modificação) de aplicações que façam uso de funcionalidades de autorização através de uma interface de programação, é proporcionar autenticação e autorização sem que sejam necessárias modificações nas aplicações existentes.

O modelo de controle de acesso adotado inicialmente aqui é, de forma similar ao observado no PERMIS, o CABP. Assim, utilizando o conceito de papéis, os privilégios

[8] A comparação completa entre o modelo proposto e o PERMIS é feita no capítulo 7.

associam-se às entidades de forma indireta, o que propicia, entre outras coisas, maior flexibilidade e menor custo administrativo.

Para que autorização e conseqüente controle de acesso aconteçam conforme as características do CABP, a existência de dois tipos de certificados de atributos se faz necessária: o Certificado de Especificação de Papel (CEP) e o Certificado de Relacionamento a Papéis (CRP) (vide subseção 4.3.4). Em relação à distribuição desses certificados, observa-se que o CEP é mantido em um repositório público, e não precisa ser distribuído. Entretanto, no que se refere ao CRP, é preciso que um modelo de distribuição de credenciais seja adotado. Aqui, a postura do modelo proposto é de que não há modelos de distribuição de credenciais melhores, apenas modelos mais adequados para uma determinada situação. Com isso, a escolha do modelo de distribuição de credenciais adotado fica a cargo da entidade que gerencia o domínio, denominada Administrador de Recursos (vide subseção 6.1.1).

Além da autenticação e da autorização, alguns serviços de segurança adicionais, listados no capítulo 7 como trabalhos futuros, também são alvos da integração entre as infra-estruturas ICP e IGP: auditoria e tempestividade. Através deles, e com o auxílio de ferramentas e procedimentos adequados, é possível a concretização, por exemplo, da reconstrução de eventos ocorridos no ambiente.

6.1. ARQUITETURA BÁSICA

A arquitetura básica do modelo proposto, representada na Figura 21, é formada por uma série de elementos, entre eles:

- **Administrador de Recursos**. Esse é o elemento humano responsável por

gerenciar a emissão e revogação dos certificados de atributos CEP e CRP. Além disso, o Administrador de Recursos é responsável por gerir a política de autorização do domínio, tratando de sua edição, emissão e publicação. Todas essas atividades são realizadas com o auxílio da Entidade de Atribuição de Privilégios.

- **Política de Autorização (PA)**. Esse elemento contém os parâmetros que devem ser considerados durante os procedimentos de atribuição de privilégios e de concessão de acesso, tais como o período máximo de tempo que a associação entre entidade final e privilégio pode durar.

- **Entidade de Atribuição de Privilégios (EAP)**. Interagindo diretamente com a Autoridade de Atributos (AA), esse elemento pode ser considerado como uma interface de acesso aos serviços de gerenciamento de certificados de atributos proporcionados pela AA. Sob o comando do Administrador de Recursos, a EAP, além de permitir a edição, emissão e publicação da PA do domínio, realiza a emissão e revogação dos certificados de atributos CEP e CRP.

- **Entidade Controladora de Aplicações (ECA)**. Esse elemento pode ser considerado como um verificador de privilégios, através do qual são realizados os processos de autorização de um domínio. Observa-se, portanto, que o objetivo principal da ECA é restringir o acesso aos recursos protegidos. Para isso, a ECA, durante as decisões de concessão de acesso, faz uso de um conjunto de informações, que engloba a PA do domínio, os certificados relacionados às entidades finais e variáveis de ambiente, tais como o momento em que a requisição de acesso se iniciou.

- **Agente Gerenciador de Certificados de Atributos (AGCA)**. Quando o modelo de apresentação for adotado como forma de distribuição de credenciais, a entidade final, através do AGCA, interage com a EAP para apresentar os certificados CRP

que devem ser considerados durante as concessões de acesso. Além disso, através do AGCA é possível que a entidade final interaja com outras entidades da arquitetura, como a EAP e AGCAs pertencentes a outras entidades finais. Ao interagir com a EAP, a entidade final solicita associações a privilégios e, durante a interação com outros AGCAs, é possível realizar-se a delegação dinâmica de privilégios entre entidades finais.

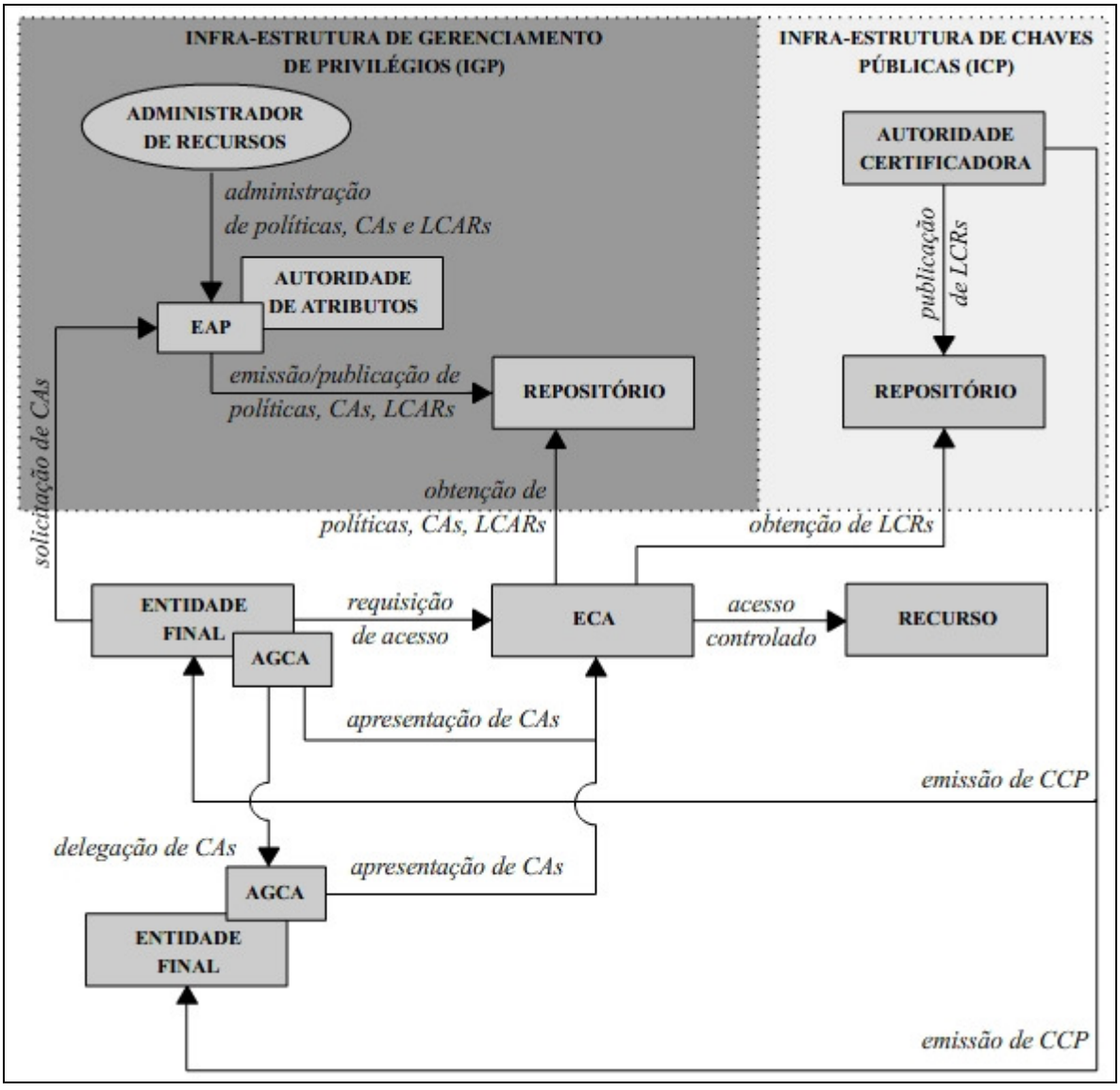

Figura 21. Arquitetura básica do modelo proposto.

Em adição aos elementos citados anteriormente, nota-se a importância de outras entidades para o funcionamento do modelo, entre eles o Repositório. Presente tanto na ICP

quanto na IGP, esse elemento é responsável por armazenar certificados (CCP ou CA), listas de certificados revogados (LCR ou LCAR) e políticas.

6.1.1. Administrador de Recursos

Vide página 60.

6.1.2. Política de Autorização

A Política de Autorização (PA), especificada sob o formato da linguagem XML, rege as atividades de autorização. Seguindo os moldes da política de autorização adotada pelo PERMIS (vide subseção 5.1.1), a PA incorpora alguns de seus elementos. Além disso, de forma similar ao observado no PERMIS, a PA é assinada digitalmente pela AA do domínio e mantida no Repositório sob a forma de um CA.

Usada pelas entidades EAP, ECA e até mesmo pelo AGCA, a PA, representada na Figura 22, tem dois objetivos principais: definir os parâmetros que devem ser considerados durante a emissão de certificados de atributos e especificar sob quais condições o acesso a um recurso deve ser concedido. No que se refere à emissão de certificados de atributos, a EAP, antes de atribuir qualquer tipo de privilégio às entidades, consulta a PA para determinar, por exemplo, o período de tempo máximo em que uma atribuição pode ser mantida, ou seja, o período de validade de um certificado. Já em relação à concessão de acesso, a ECA consulta a PA para determinar se os privilégios apresentados por uma entidade são suficientes para acessar um determinado recurso.

```
<PA id="PA01">

  <ListaDominiosICP>
    <DominioICP id="ac-raiz">
      <Exclui campo="PropositoChave" valor="Assinatura de código">
      <Inclui campo="NomeEmissor" valor="CN=AC Raiz">
    </DominioICP>
  </ListaDominiosICP>

  <ListaPapeis>
    <Papel id="admin" valor="administrador" />
    <Papel id="usr" valor="usuario" />
  </ListaPapeis>

  <ListaAssociacoesDominiosPapeis>
    <AssociacaoDominioPapel dominioICP="ac-raiz" papel="usr">
      <Validade horas="24" />
      <Delegacao limite="1" />
    </AssociacaoDominioPapel>
    <AssociacaoDominioPapel dominioICP="ac-raiz" papel="admin">
      <Validade horas="12" />
      <Delegacao limite="-1" />
      <Revogacao criticidade="1" distribuicao="ldap:10.0.10.2:389" />
    </AssociacaoDominioPapel>
  </ListaAssociacoesDominiosPapeis>

  <ListaRecursos>
    <Recurso id="servidorWeb01" endereco="10.0.0.10:80" />
  </ListaRecursos>

  <ListaAssociacoesPapeisRecursos>
    <AssociacaoPapelRecurso recurso="servidorWeb01" papel="usr">
      <Intervalo inicio="09:00" termino="18:00" />
      <Revogacao criticidade="0" />
    </AssociacaoPapelRecurso>
  </ListaAssociacoesPapeisRecursos>

</PA>
```

Figura 22. Política de Autorização.

6.1.2.1. Domínios ICP

A Política de Autorização, através da lista de domínios ICP (elemento `ListaDominiosICP`), define que apenas determinados conjuntos de entidades finais são elegíveis à emissão de certificados de atributos. A cada um desses conjuntos, denominados

domínios ICP, são aplicados mecanismos de filtragem que têm por objetivo restringir o número de participantes do domínio.

A filtragem é feita com base nos campos pertencentes ao certificado de chave pública (CCP) relacionado a cada entidade final. Cada um dos filtros aplicados é definido pelos elementos `Exclui` e `Inclui`, que possuem dois atributos, `campo` e `valor`. O atributo `campo` faz correspondência direta com os campos do certificado de chave pública da entidade final (vide subseção 2.2) que devem ser analisados a fim de determinar se o valor contido é o mesmo especificado pelo atributo `valor`. Durante a filtragem, o comportamento padrão é o de exclusão. Com isso, caso o resultado de um único filtro de exclusão seja verdadeiro, o domínio ICP sendo analisado é descartado para a entidade em questão.

6.1.2.2. Papéis

Através do elemento `ListaPapeis` é possível definir o conjunto de papéis que pode ser associado aos domínios ICP. Cada um dos elementos formadores desse conjunto é descrito pelo elemento `Papel` que, além de possuir um identificador único, possui um valor associado.

6.1.2.3. Associações entre domínios ICP e papéis

Só é feita a associação entre uma entidade final e um papel caso, dentro da lista de relacionamentos entre domínios ICP e papéis (definida pelo elemento `ListaAssociacoesDominiosPapeis`), sejam satisfeitas as seguintes condições:

- existência, dentro de uma associação qualquer, de um papel que esteja associado a

um domínio ICP concordante com o domínio determinado nos procedimentos de filtragem de domínios (vide subseção 6.1.2.2);

- existência, dentro da mesma associação, de um papel que esteja em concordância com o papel selecionado pelo Administrador de Recursos (vide subseção 6.1.2.3).

Caso ambas as condições citadas anteriormente sejam satisfeitas, a EAP emite para a entidade final um CA que atenda às restrições impostas pelos elementos `Validade`, `Delegação` e `Revogação`. Através deles é possível, respectivamente, limitar o período de validade do CA, restringir a capacidade de delegação posterior e impor características de checagem de revogação.

6.1.2.4. Recursos

Através do elemento `ListaRecursos` é possível definir-se o conjunto de recursos a serem protegidos.

6.1.2.5. Associações entre papéis e recursos

O acesso a um recurso só é permitido se, dentro da lista de associações definida pelo elemento `ListaAssociacoesPapeisRecursos`, houver, para o recurso em questão, uma associação cujo papel relacionado esteja em concordância com o papel ao qual a entidade final está associada.

6.1.3. Entidade de Atribuição de Privilégios

Sob responsabilidade do Administrador de Recursos do domínio está a atribuição de privilégios às entidades finais. No modelo proposto, atribuir privilégios a uma entidade significa associá-la a um papel através da emissão de um CRP. Aqui, a emissão e conseqüente revogação de um CRP são realizadas pela Entidade de Atribuição de Privilégios (EAP) que pode ser considerada como uma interface de acesso aos serviços de gerenciamento de certificados de atributos proporcionados pela AA. Observa-se que a EAP, além de interagir com a AA, interage, conforme ilustrado na Figura 23, com uma série de outros elementos.

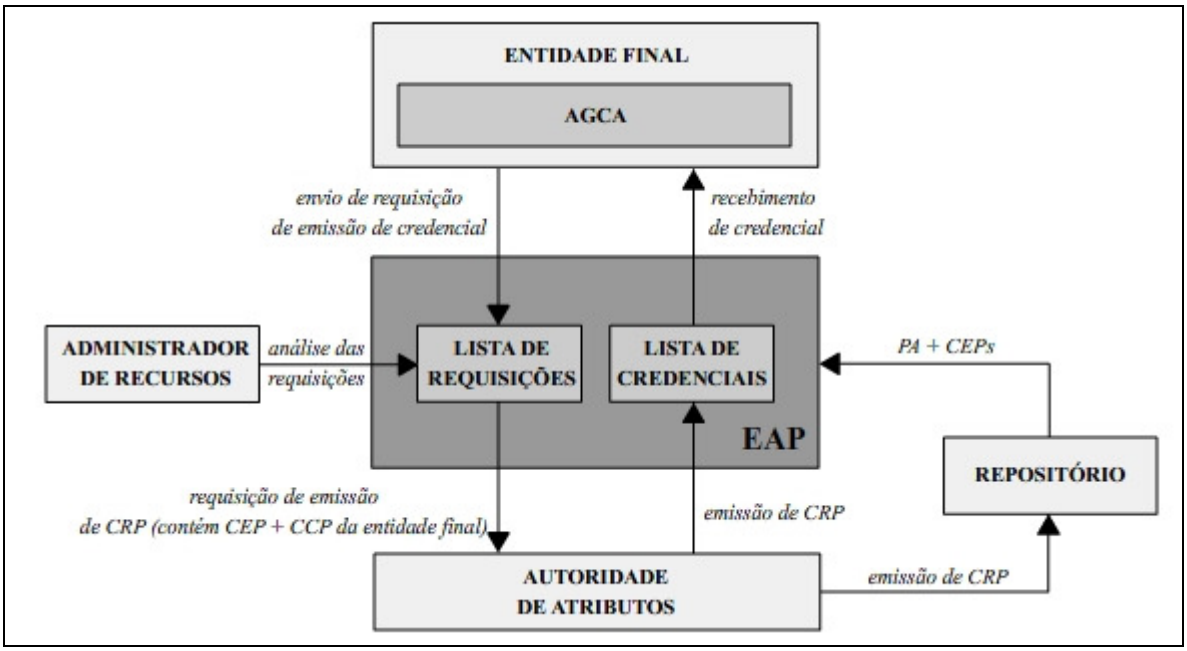

Figura 23. Entidade de Atribuição de Privilégios.

O objetivo principal da EAP é proporcionar ao Administrador de Recursos uma interface centralizada de gerenciamento de privilégios. Através dela, é possível, por exemplo, controlar os privilégios associados aos papéis. No entanto, seu principal benefício está associado ao fato de que, por intermédio de suas funcionalidades, é possível o gerenciamento dos privilégios associados às entidades finais. Para isso, na composição da EAP, há dois

elementos de grande destaque: a Lista de Requisições, que armazena, temporariamente, todos os pedidos de associação a papéis oriundos das entidades finais, e a Lista de Credenciais que, também em caráter temporário, armazena uma série de informações[9] relacionadas aos CRPs emitidos para as entidades finais[10].

Ambas as listas, conforme observado na Figura 24, além de muito semelhantes, estão interligadas através do campo `ID_REQ`, que armazena um número único para cada uma das requisições existentes.

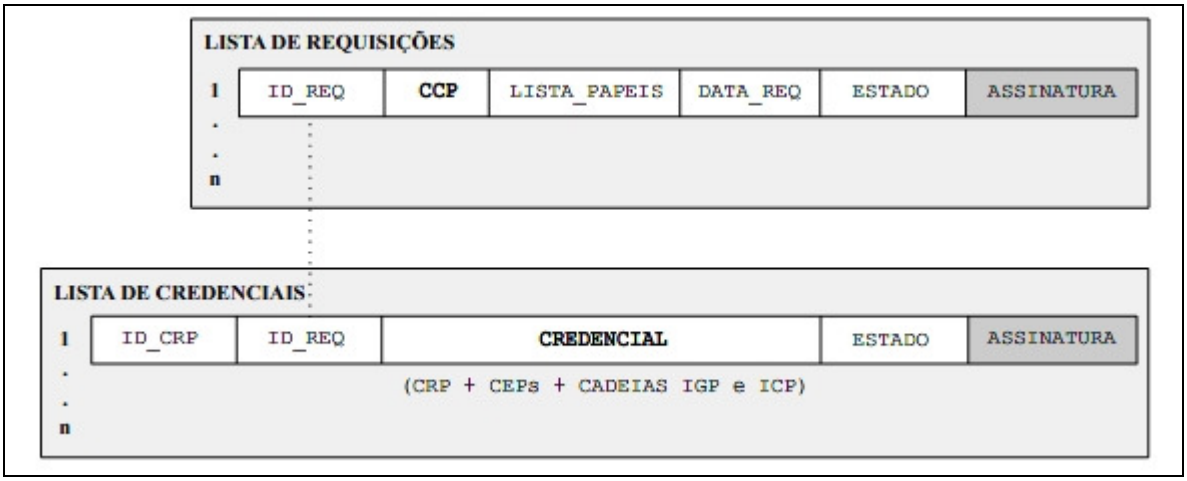

Figura 24. Lista de Requisições e Lista de Credenciais.

A Lista de Requisições é composta pelos seguintes elementos:

- `ID_REQ`, que, conforme dito anteriormente, armazena um número único para cada uma das requisições existentes;
- `CCP`, que guarda o certificado de chave pública pertencente à entidade final da qual se originou a requisição;

---

[9] Observa-se que nas ilustrações posteriores, o conjunto de informações relacionadas ao CRP é denominado credencial. Cada credencial é forma pelo CRP, pelos CEPs, pelas cadeias IGP e pelas cadeias ICP associadas.

[10] O tempo de permanência dos registros nessas listas é definido pelo Administrador de Recursos.

- LISTA_PAPEIS, que armazena os nomes dos papéis selecionados pela entidade final;
- DATA_REQ, que guarda o momento em que a requisição foi recebida;
- ESTADO, que indica a situação em que a requisição se encontra: "**Em análise**", "**Rejeitada**" ou "**Aprovada**";
- ASSINATURA, que contém a assinatura digital realizada pela EAP, tendo como base todas as informações contidas nos campos anteriores. O principal objetivo dessa assinatura é proporcionar integridade de cada um dos registros existentes na lista.

Já a Lista de Credenciais é formada pelos seguintes elementos:

- ID_CRP, que armazena um número único para cada uma dos registros existentes;
- ID_REQ, que faz referência à requisição que deu origem ao CRP emitido;
- CREDENCIAL, que, além de armazenar o certificado de relacionamento a papéis emitido para a entidade final, armazena também uma série de outras informações: as cadeias de certificados CRP, cadeias de certificação ICP e CEPs aos quais o CRP faz referência;
- ESTADO, que indica a situação em que a credencial se encontra no que se refere ao envio para a entidade final: "**Pendente de envio**", ou "**Enviado**";
- ASSINATURA, que contém a assinatura digital realizada pela EAP, tendo como base todas as informações contidas nos campos anteriores. O principal objetivo dessa assinatura é proporcionar integridade de cada um dos registros existentes na lista.

Além de concentrar as informações de atribuição de privilégios, a EAP oferece ao

Administrador de Recursos uma outra facilidade: o gerenciamento da PA, que envolve atividades de edição, emissão e publicação.

6.1.4. Entidade Controladora de Aplicações

Semelhante ao subsistema de verificação de privilégios do PERMIS, a Entidade Controladora de Aplicações (ECA) é responsável por autenticar e autorizar as entidades finais durante as requisições de acesso a recursos. Para isso, a ECA, ilustrada na Figura 25, age como um filtro, interceptando todas as requisições de acesso aos recursos protegidos originadas das entidades finais.

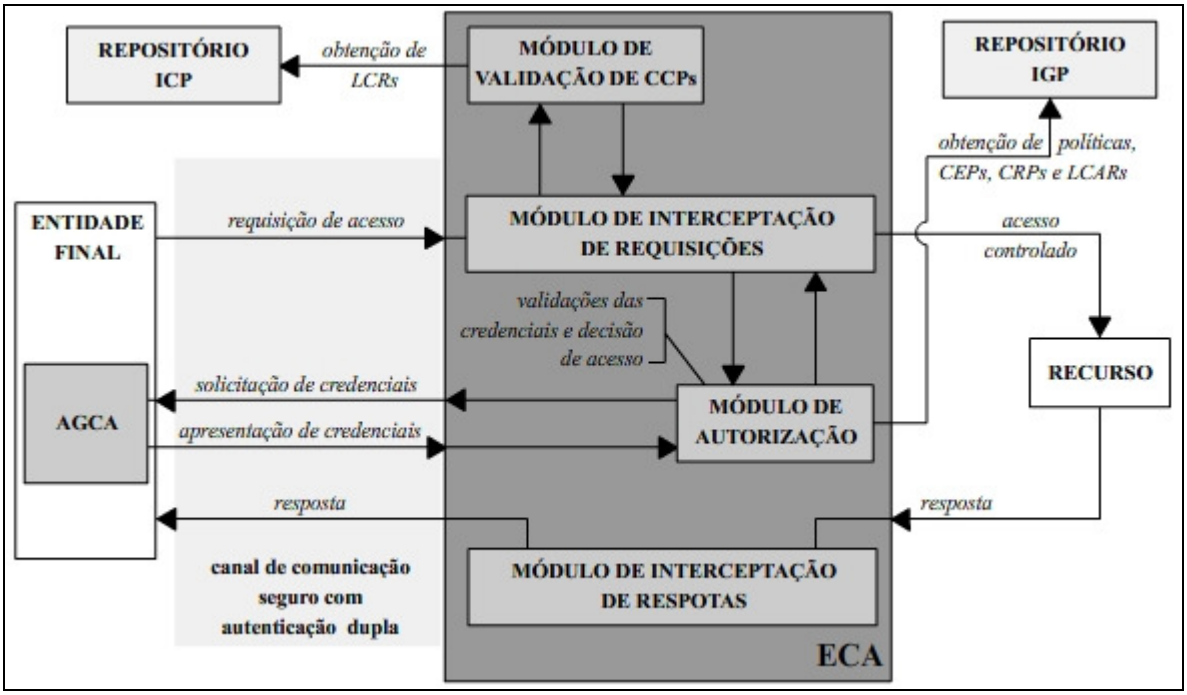

Figura 25. Entidade Controladora de Aplicações.

Uma das premissas do modelo proposto é de que os protocolos de acesso aos recursos protegidos suportem, além do serviço de procuração (serviço *proxy*) das sessões de comunicação, o estabelecimento de canais de comunicação seguros com autenticação dupla.

Utilizando as técnicas observadas nos protocolos *Secure Sockets Layer* (SSL) (FREIER; KARLTON; KOCHER, 1996) e *Transport Layer Security* (TLS) (DIERKS; ALLEN,1999), por exemplo, faz-se possível estabelecer um canal de comunicação que proporcione, entre outras coisas, integridade e sigilo das informações trafegadas. Com isso, a cada requisição de acesso a um recurso protegido, é preciso que a entidade final e a ECA troquem, a fim de estabelecer um canal de comunicação seguro, uma série de informações. Então a ECA, após fazer todas as validações de autenticação e autorização necessárias, pode interagir, em nome da entidade final, com o recurso em questão. Não há, sob qualquer circunstância, estabelecimento direto de comunicação entre a entidade final e o recurso.

Para que as validações de autenticação e autorização realizadas pela ECA realmente sejam postas em prática, o primeiro passo a ser dado pela própria ECA é a interpretação da PA do domínio. Visto que um dos objetivos da PA é especificar sob quais condições o acesso a um recurso deve ser concedido, ela serve como uma das bases para o processo de controle de acesso.

Em relação à autenticação, a ECA, após obter o CCP pertencente à entidade final do próprio canal de comunicação estabelecido entre elas, efetua diversas checagens ligadas a esse certificado:

- integridade da assinatura digital contida no certificado;
- validade do certificado;
- integridade e validade da cadeia de certificação;
- propósito da chave;
- revogação.

Em relação à autorização, a ECA, de forma semelhante ao observado para a autenticação, realiza uma série de checagens para os CRPs relacionados às entidades finais.

Essas checagens são independentes do modelo de distribuição de credenciais escolhido e se aplicam igualmente para todos os CRPs. A principal diferença entre as verificações realizadas durante a autenticação e durante a autorização refere-se ao fato de que a estrutura de um CRP, ao contrário do observado para um CCP, não possui campos que suportem o armazenamento de uma chave pública. Com isso, uma das checagens mais relevantes durante a autorização diz respeito à validade da correspondência do CRP com o CCP apresentado durante a autenticação.

Todas essas validações servem como pré-requisito para que a ECA, através da interpretação da PA, determine se o contexto da requisição formado pelos certificados relacionados à entidade final, características do recurso em questão e variáveis de ambiente, é suficiente para que o acesso ao recurso protegido se realize.

6.1.5. Agente Gerenciador de Certificados de Atributos

O Agente Gerenciador de Certificados de Atributos (AGCA) auxilia a entidade final na execução de atividades administrativas e operacionais apenas quando o modelo de distribuição de credenciais observado na subseção 3.2.1 for adotado. Dessa forma, o AGCA não é utilizado em conjunto com o modelo de obtenção de credenciais. Seu objetivo, portanto, é proporcionar facilidades para que as entidades finais realizem as seguintes tarefas:

- solicitação de emissão de CRPs (através da interação com a EAP);
- apresentação de CRPs à ECA;
- delegação de CRPs a outras entidades.

Para que a delegação de CRPs seja possível, as entidades envolvidas no processo de

delegação se comunicam conforme ilustra a Figura 26. Nota-se que o AGCA da entidade que delega o CRP, de forma semelhante à EAP, contém a Lista de Requisições e a Lista de Credenciais. Ambas as listas possuem o mesmo formato observado para a EAP.

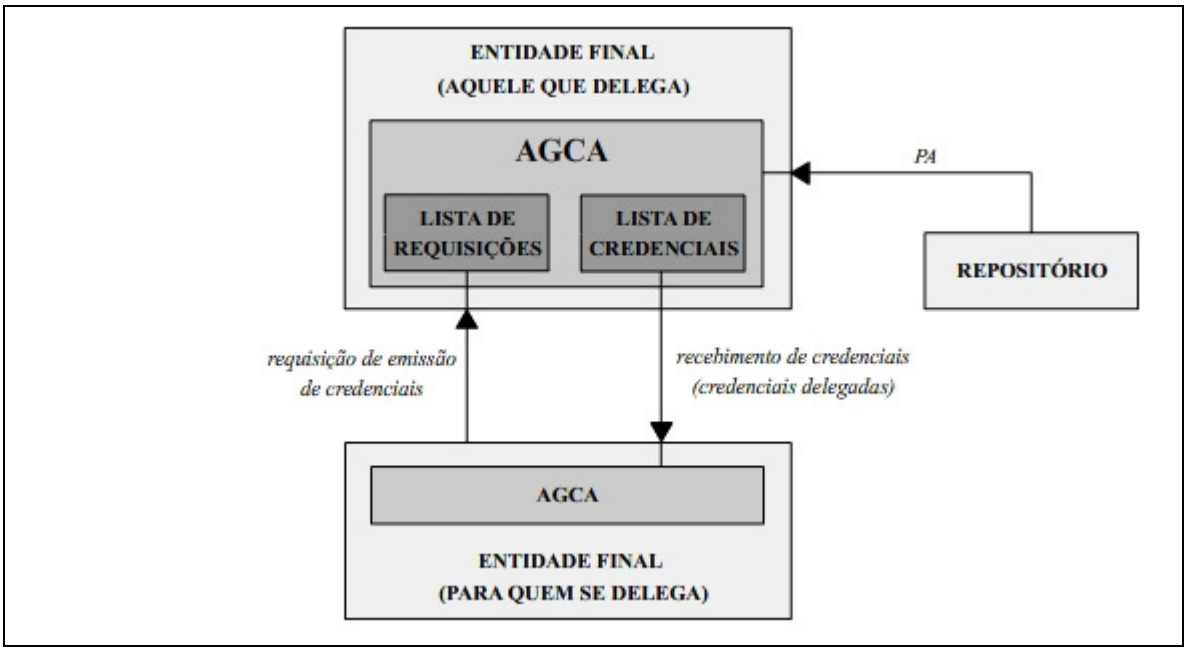

Figura 26. O Agente Gerenciador de Certificados de Atributos e a delegação de privilégios.

6.2. PROTOCOLOS DE COMUNICAÇÃO

Para que as tarefas listadas na subseção 6.1.5 sejam executadas, o AGCA interage diretamente com as demais entidades através dos seguintes protocolos de comunicação:

- Protocolo de Solicitação de Privilégios (PSP), utilizado na interação entre AGCA e EAP para a solicitação de emissão de um CRP;
- Protocolo de Apresentação de Credenciais (PAC), utilizado na interação entre ECA e AGCA para a apresentação de CRPs;
- Protocolo de Delegação de Privilégios (PDP), utilizado na interação entre AGCAs

para a delegação de um CRP.

As mensagens desses protocolos têm seu formato baseado na linguagem XML, e a sua transmissão é feita com o auxílio do *Hypertext Transfer Protocol* (HTTP) encontrado em Fielding et al (1999).

6.2.1. Protocolo de Solicitação de Privilégios

No modelo proposto, a associação a um privilégio se traduz na emissão de um CRP. Entretanto, para que um certificado dessa natureza seja emitido, é preciso, inicialmente, que as entidades finais selecionem o conjunto de papéis aos quais desejam se afiliar através do Protocolo de Solicitação de Privilégios (PSP) ilustrado na Figura 27.

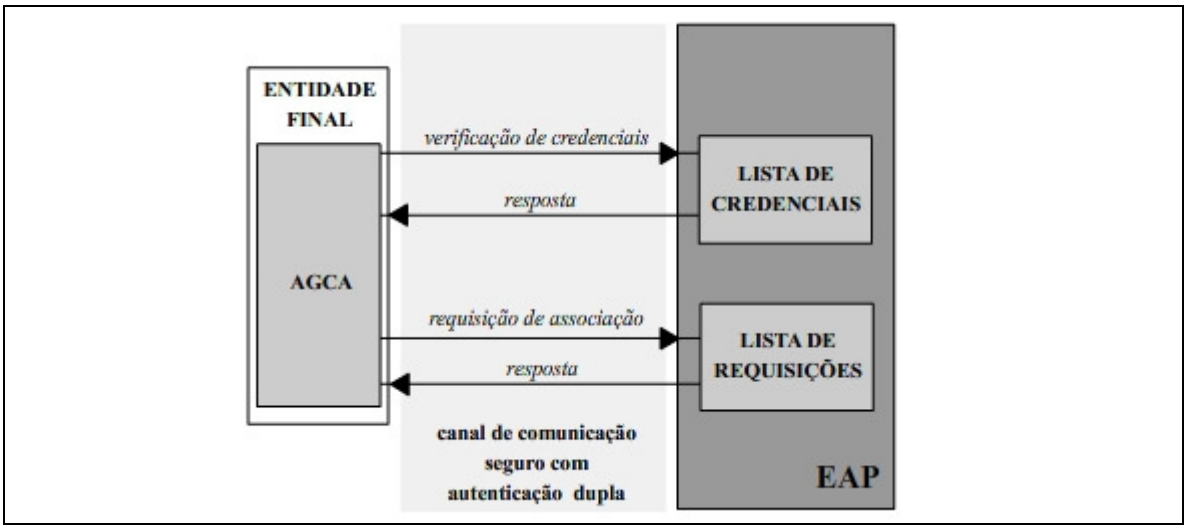

Figura 27. Protocolo de Solicitação de Privilégios.

No primeiro passo do PSP, a entidade final, por intermédio do AGCA, envia para a EAP uma mensagem simples, ilustrada na Figura 28, que tem por objetivo verificar se na Lista de Credenciais há algum CRP recentemente emitido.

```
<Requisicao>
  <Funcao nome="VerficaListaCredenciais" />
</Requisicao>
```

Figura 28. Mensagem de verificação de existência de CRPs na Lista de Credenciais.

A resposta para essa requisição, ilustrada na Figura 29, encapsula, sempre utilizando a codificação Base 64 (LINN, 1993; FREED; BORENSTEIN, 1996), uma série de informações referentes a um CRP: cadeias de certificados CRP, cadeias de certificação ICP e CEPs aos quais o CRP se associa. Essas informações são utilizadas para o acesso a um recurso protegido, e, por isso, durante um intervalo de tempo baseado no período de vida do próprio CRP, são mantidas pela entidade final.

```
<Resposta>
  <ListaCredenciais>
    <Credencial id="C01">
      <CRP>
        <CA>MII5LKCWE5Q...ASD5R==</CA>
        <CadeiaIGP>
          <Emissor>
            <CA>MII5LKCWE5Q...ASD5R==</CA>
            <CCP>MIICXfCCA...QWT3</CCP>
            <CadeiaICP>
              <CCP>MIICXTCCA...41AR</CCP>
              ...
            </CadeiaICP>
          </Emissor>
          ...
        </CadeiaIGP>
      </CRP>
      <ListaCEPs>
        <CEP>
          <CA>MII5LKCEQ7Y...4HXZ8==</CA>
          <Emissor>
            <CCP>MIICXfCCA...QWT3</CCP>
            <CadeiaICP>
              <CCP>MIICXTCCA...41AR</CCP>
              ...
            </CadeiaICP>
          </Emissor>
        </CEP>
        ...
      </ListaCEPs>
    </Credencial>
    ...
  </ListaCredenciais>
</Resposta>
```

Figura 29. Resposta para a função de verificação de existência de CRP na lista.

Observa-se que a operação de recebimento de CRPs é vital para o modelo de apresentação de credenciais adotado. Portanto, é preciso que a entidade final, através do AGCA, envie uma mensagem de confirmação de recebimento dos CRPs, conforme ilustrado na Figura 30.

```
<Confirmacao>
  <Funcao nome="ConfirmaRecebimento" />
  <ListaCredenciais>
    <Credencial id="C01" />
    <Credencial id="C02" />
    ...
  </ListaCredenciais>
</Confirmacao>
```

Figura 30. Confirmação de recebimento de CRPs.

Supondo que a entidade final deseje então se associar a algum papel, a mensagem ilustrada na Figura 31 é enviada para a EAP.

```
<Requisicao>
  <Funcao nome="CriaCRP" />
  <ListaPapeis>
    <Papel id="P01" valor="usr" />
    <Papel id="P02" valor="admin" />
    ...
  </ListaPapeis>
</Requisicao>
```

Figura 31. Requisição de associação a papéis.

A EAP então interpreta a PA do domínio e determina se, para aquela entidade final, as associações solicitadas são autorizadas. Em caso positivo, a EAP cria um registro na Lista de Requisições e, na montagem da resposta, representada na Figura 32, adiciona o estado "**Requisição inserida**". Esse novo registro ainda não é um CRP. Trata-se apenas de uma requisição de associação pendente de aprovação. Caso o Administrador de Recursos, em análises posteriores, determine que a requisição seja válida, a EAP interage com a AA e emite um CRP. Do contrário, não é inserido registro algum na Lista de Requisições e o estado relacionado àquela associação é definido como "**Associação não permitida**".

```
<Resposta>
  <ListaPapeis>
    <Papel id="P01" status="Requisição inserida" />
    <Papel id="P02" status="Associação não permitida" />
    ...
  </ListaPapeis>
</Resposta>
```

Figura 32. Resposta para a função de associação a papéis.

6.2.2. Protocolo de Apresentação de Credenciais

Quando a distribuição de credenciais faz-se de acordo com o modelo de apresentação, é necessário que a entidade final, em meio a uma requisição de acesso a um recurso protegido, apresente à ECA todos os CRPs que devem ser considerados para a formação do contexto de acesso. Essa apresentação de CRPs é feita com o auxílio do Protocolo de Apresentação de Credenciais (PAC), ilustrado na Figura 33.

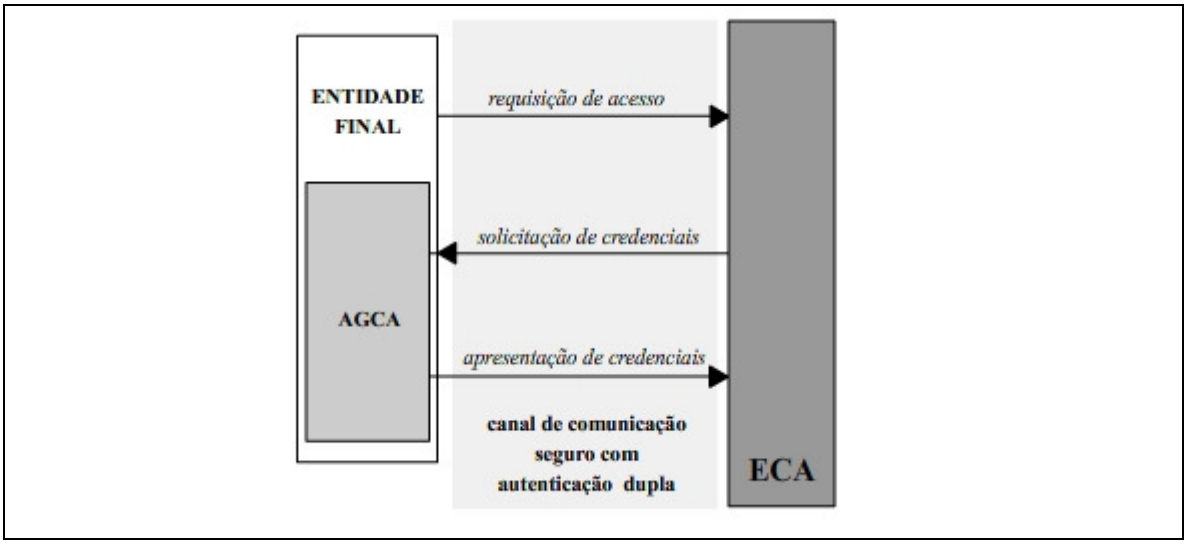

Figura 33. Protocolo de Apresentação de Privilégios.

O PAC é iniciado pela ECA que, durante os procedimentos de determinação do contexto de acesso de uma requisição, solicita à entidade final os CRPs a serem considerados.

Essa solicitação é feita através do envio, por parte da ECA, de uma mensagem simples, conforme ilustrado na Figura 34.

```
<Requisicao>
  <Funcao nome="SolicitaCRP" />
</Requisicao>
```

Figura 34. Mensagem de solicitação de CRPs.

Após receber essa mensagem, o AGCA interage com o usuário final, que então seleciona um ou mais CRPs. Em seguida, esses certificados, juntamente com os CEPs referentes, cadeias de CRPs e cadeias ICP, são encapsulados na mensagem, conforme ilustrado na Figura 29, e enviados para a ECA.

6.2.3. Protocolo de Delegação de Privilégios

Ilustrado na Figura 35, o Protocolo de Delegação de Privilégios (PDP) segue os mesmos passos do PSP. A única diferença é que apenas as entidades finais, através de seus AGCAs, participam do PDP.

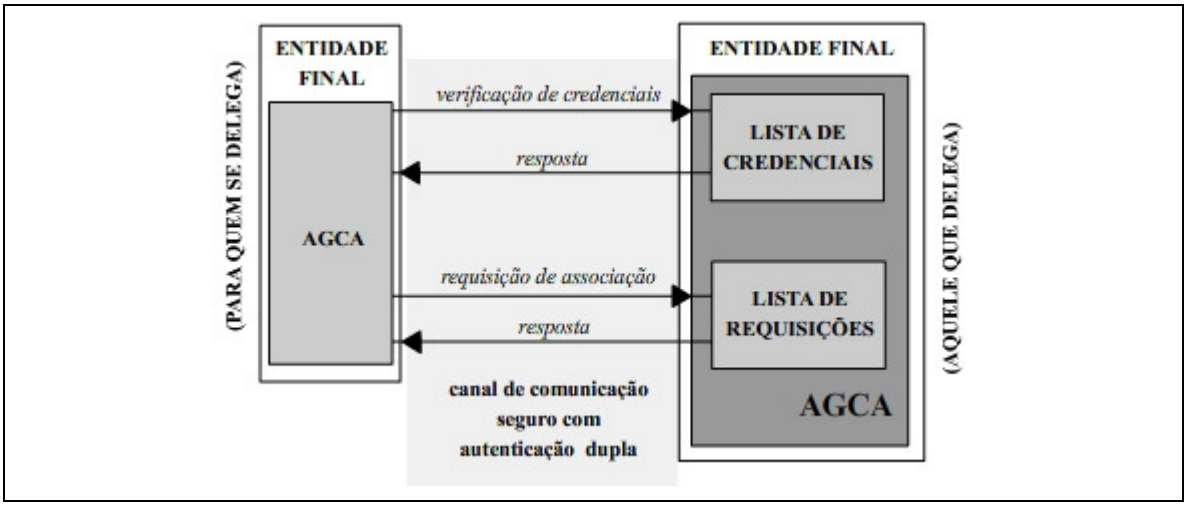

Figura 35. Protocolo de Delegação de Privilégios.

6.3. REVOGAÇÃO

Em alguns ambientes, o período de validade de um CA é menor do que o tempo requerido para emissão e distribuição de informações de revogação (FARRELL; HOUSLEY, 2002). Nessas situações, a existência de mecanismos de suporte à revogação é incomum. Entretanto, em algumas situações de alto risco, como, por exemplo, transferências bancárias, a existência de mecanismos de revogação, mesmo para CAs com curtos períodos de vida, é um importante requisito de segurança. Sendo assim, para tratar a revogação na IGP, há duas opções:

- a revogação pode ser ignorada: durante o processo de emissão de um CA, a AA, através da extensão `noRevAvail`, indica aos verificadores de privilégios que a checagem da revogação é um item sem importância;
- a revogação pode ser crítica: de forma similar ao observada para os CCPs, é possível que um dos campos de um CA aponte para os locais onde a informação de revogação é distribuída. Geralmente, a distribuição das informações de revogação é feita com o auxílio de uma LCAR, armazenada em um repositório central.

Para o modelo proposto, a exemplo do observado na escolha da forma de distribuição de credenciais, adota-se a postura de que o melhor esquema de revogação é aquele que melhor se adequa às necessidades do ambiente. A escolha do mecanismo adotado fica sob responsabilidade do Administrador de Recursos do domínio.

6.4. MODELOS DE FUNCIONAMENTO

Diretamente relacionado à forma de distribuição de credenciais adotada, o funcionamento do modelo aqui proposto é classificado em duas categorias:

- Modelo de apresentação de credenciais: no qual, durante os processos de autorização, os CRPs associados à entidade final são obtidos através da interação entre ECA e AGCA;
- Modelo de obtenção de credenciais: no qual, durante os processos de autorização, os CRPs são obtidos pela ECA através de uma consulta ao Repositório, sem que haja interação com a entidade final.

Observa-se que apenas um formato de funcionamento pode ser escolhido. Um modelo híbrido que suporte, ao mesmo tempo, a distribuição e a obtenção de credenciais não é suportado.

6.4.1. Modelo de apresentação de credenciais

Nesse modelo, cuja arquitetura é representada na Figura 36, os processos de autorização exigem participação direta da entidade final que, através do AGCA, interage com a ECA por meio do protocolo PAC observado em 6.2.2.

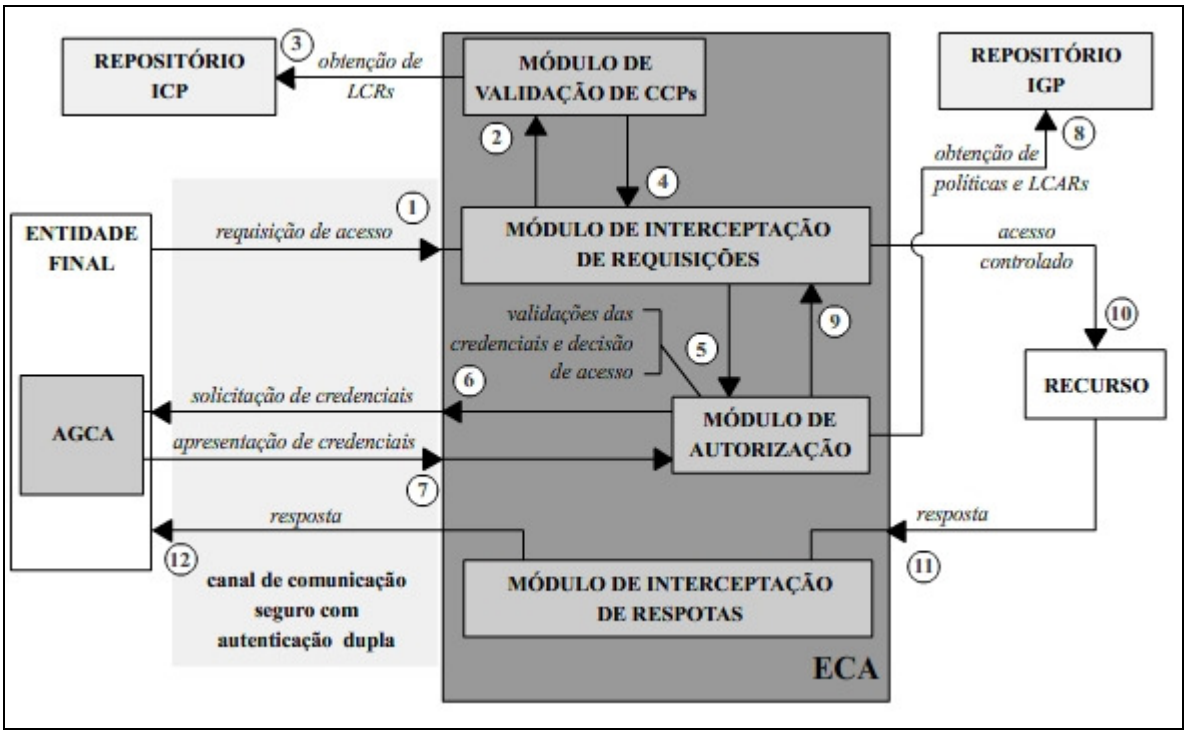

Figura 36. Arquitetura do modelo de apresentação de credenciais.

Inicialmente, conforme indica o passo 1, a entidade final envia uma requisição de acesso a um recurso protegido. Essa solicitação é encapsulada de acordo com o protocolo nativo da aplicação que, como premissa, deve suportar o serviço de procuração das sessões de comunicação (serviço *proxy*) e o estabelecimento de canais de comunicação seguros com autenticação dupla. Isso significa que, para acessar uma aplicação *web*, por exemplo, é preciso que o protocolo de acesso HTTP *over* TLS (HTTPS), encontrado em Rescorla (2000).

Em seguida, a requisição é tratada pela ECA que, durante o estabelecimento do canal seguro de comunicação, solicita à entidade final a apresentação de seu CCP através das técnicas observadas em Dierks e Allen (1999), por exemplo. Inicia-se, portanto, o processo de autenticação, que depende diretamente do resultado das checagens feitas sobre o CCP apresentado pela entidade final (vide passos 2 e 3). Caso o resultado dessas validações, listadas na subseção 6.1.4, seja negativo, a requisição é descartada. Do contrário, o processo de autorização pode ser iniciado.

O processo de autorização envolve o protocolo PAC que, de acordo com o observado na subseção 6.2.2, permite que a ECA, para fins de solicitação de credenciais, interaja, através do AGCA, com a entidade final. Com ele, a entidade final apresenta, através de mensagens XML, os CRPs que devem ser considerados pela ECA para a determinação do contexto de acesso (vide passos 6 e 7). Nesse ponto, a ECA, após receber o conjunto de CRPs, realiza, para cada um dos elementos desse conjunto, uma série de validações, entre elas:

- verificação de sua correspondência com o CCP apresentado durante a autenticação;
- verificação da integridade e validade da cadeia de certificação;
- verificação de sua correspondência com o CEP.

Grande parte das informações necessárias para a realização dessas checagens já está presente na mensagem de apresentação de CRPs enviada pela entidade final. Dessa forma, a ECA só obtém informações adicionais se algum mecanismo de revogação tiver sido adotado.

Observa-se que, se o resultado de alguma dessas validações for negativo, o CRP em questão é descartado. Caso todos os CRPs se enquadrem nessa condição, a requisição de acesso ao recurso protegido é rejeitada. Do contrário, a ECA continua o processo de autorização e, comunicando-se com o Repositório, obtém a PA do domínio.

Com base nas informações obtidas nos passos anteriores, a ECA analisa a PA a fim de determinar se, para o recurso protegido em questão, a combinação formada pelo CCP da entidade final, os CRPs (e CEPs) associados, e variáveis de ambiente, tais como o momento da requisição, formam um contexto suficiente para que o acesso seja permitido (vide passo 9). Se esse contexto for suficiente, a ECA inicia a comunicação com o recurso protegido (vide passo 10) e, ao longo de todas as operações realizadas pela entidade final, age como mediador entre entidade final e recurso protegido.

6.4.2. Modelo de obtenção de credenciais

Em ambientes que tenham por objetivo isentar a entidade final da responsabilidade do gerenciamento de credenciais, a interação entre a entidade final e a ECA, no que se refere à apresentação de credenciais, pode ser indesejada. Ambientes como esses requerem que ECA, durante os processos de autorização, obtenha os CRPs relacionados à entidade final de outra forma que não através da comunicação com o AGCA. Esse modelo de funcionamento, representado na Figura 37, exige, portanto, que os CRPs emitidos para as entidades finais sejam armazenados no Repositório, juntamente com os CEPs e com a PA do domínio.

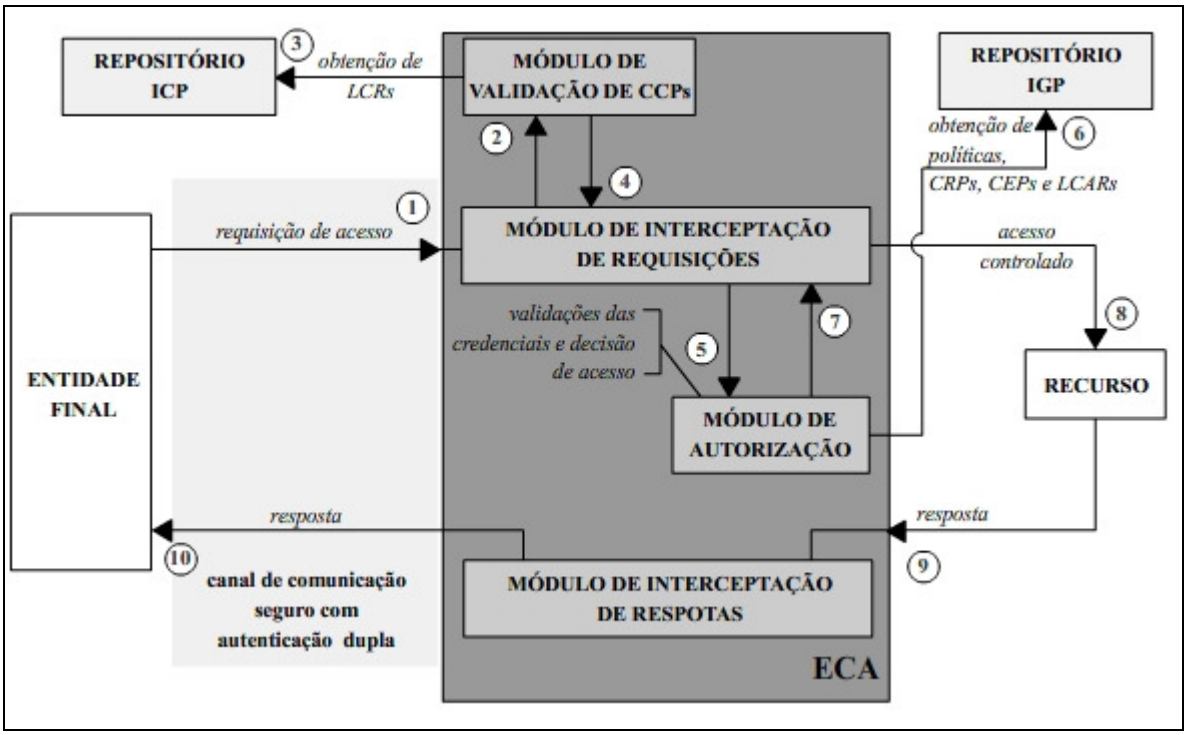

Figura 37. Arquitetura do modelo de obtenção de credenciais.

A principal diferença entre esse modelo e o modelo encontrado na subseção 6.2.1 é que, durante a autorização, a ECA não interage com o AGCA localizado na entidade final. Ao invés disso, a ECA consulta o repositório para determinar quais CRPs serão considerados para a formação do contexto de acesso da requisição (vide passo 6). Os passos remanescentes são

os mesmos.

6.4.3. Comparação entre os modelos

Ao compararem-se os modelos de funcionamento apresentados anteriormente, pode-se constatar que a principal vantagem oferecida pelo modelo de apresentação de credenciais está relacionada à forma como as cadeias de certificação são tratadas. Em meio às requisições de acesso aos recursos protegidos, a entidade final apresenta à ECA não só os CRPs, mas também um conjunto de informações relacionadas que engloba CEPs, cadeias de CRPs e cadeias de certificação ICP. Com isso, a ECA consulta o Repositório apenas para obter a PA do domínio e as informações de revogação.

Uma outra vantagem proporcionada pelo modelo de apresentação, a delegação, também está relacionada à forma como as informações de autorização são apresentadas pela entidade final à ECA. Uma vez que a entidade final apresenta à ECA todo o conjunto de informações referentes à delegação do CRP, a tarefa de descoberta do caminho de delegação tem sua complexidade reduzida.

Já o modelo de obtenção de credenciais, embora isente a entidade final de qualquer responsabilidade pelo gerenciamento das informações de autorização, sobrecarrega a ECA, que passa a acumular uma série de tarefas.

6.5. PREMISSAS DO MODELO

Para que o modelo proposto seja aplicável tanto para o modelo de apresentação quanto

para o modelo de obtenção de credenciais, as seguintes premissas devem ser atendidas:

- o domínio de recursos a serem protegidos deve ser resguardado de forma a estar localizado em um segmento de rede separado, ao qual apenas a ECA possua acesso. Não é permitida a comunicação direta entre entidade final e recurso, e toda requisição de acesso deve ser tratada pela ECA;
- os protocolos de acesso aos recursos protegidos devem suportar o serviço de procuração das sessões de comunicação (serviço *proxy*) e o estabelecimento de canal seguro de comunicação com autenticação dupla;
- no tocante ao gerenciamento dos CCPs, deve existir uma infra-estrutura ICP formada, minimamente, por uma AC capaz de gerenciar o ciclo de vida de um certificado desde sua emissão até sua possível revogação. Em adição, deve existir um repositório para o armazenamento das informações de revogação (LCRs);
- o Administrador de Recursos do domínio é o único elemento responsável por gerenciar os CEPs. Todos os CEPs do domínio devem ser publicados em um repositório central ao qual a ECA possua acesso;
- a edição, emissão e publicação da PA e o gerenciamento dos CRPs emitidos para as entidades finais também são de responsabilidade do Administrador de Recursos. Caso o modelo de obtenção de credenciais seja adotado, a AA, ao emitir os CRPs, deve publicá-los em um repositório público ao qual a ECA possua acesso;
- se o modelo de apresentação for escolhido como forma de distribuição de credenciais, a entidade final deve possuir o AGCA.

6.6. IMPLEMENTAÇÃO

A etapa de construção da prova de conceito do modelo proposto foi definida pela criação de dois protótipos, um para o modelo de funcionamento com apresentação de credenciais, e outro para o modelo de obtenção. Para ambos os protótipos, as seguintes restrições de implementação podem ser observadas:

- as informações relacionadas aos recursos que são utilizadas para a determinação do contexto de acesso estão restritas apenas aos endereços de rede. As ações que podem ser realizadas sobre os recursos não são levadas em consideração. Dessa forma, a concessão de acesso limita-se a considerar os relacionamentos entre entidades, papéis e recursos;
- devido à tecnologia utilizada para a construção da ECA, denominada *Servlet* (JAVA SERVLET TECHNOLOGY, 2005), um único protocolo de acesso a aplicações pode ser tratado pela arquitetura: o HTTP (FIELDING et al, 1999). Além disso, observa-se que o HTTP atende a uma das principais premissas do modelo proposto, que diz que os protocolos de acesso às aplicações devem suportar o serviço de procuração das sessões de comunicação (serviço *proxy*) e o estabelecimento de canal seguro de comunicação com autenticação dupla.

Os protótipos foram construídos usando-se a linguagem de programação Java, com o auxílio das bibliotecas criptográficas encontradas em IAIK Crypto Toolkits (2005). Essas bibliotecas permitem, entre outras coisas, que o tratamento de certificados de atributos seja feito de forma simples. Já para o tratamento das mensagens XML trocadas durante a execução dos protocolos PSP, PAC e PDP, utilizou-se a biblioteca *Xerces*, encontrada em Xerces Project (2005).

Utilizando a tecnologia de *Serlvets* (JAVA SERVLET TECHNOLOGY, 2005), adotada para a construção da ECA, a EAP, embora presente em ambos os protótipos, possui responsabilidades ligeiramente diferentes para cada um deles. Nos dois protótipos, a EAP interage com o Repositório através do protocolo LDAP (YEONG; HOWES; KILLE, 1995) para publicar a PA e os CEPs. No entanto, apenas para o protótipo de obtenção de credenciais, a EAP comunica-se com o Repositório para publicar CRPs. Já para o protótipo de apresentação de credenciais, a EAP, com o objetivo de manter a Lista de Requisições e a Lista de Credenciais, faz interface com um gerenciador de banco de dados (MICROSOFT SQL SERVER, 2005).

No que se refere à entidade final, o AGCA pode ser executado em quase qualquer ambiente, desde que este possua suporte à execução de código Java. O AGCA é encontrado apenas no protótipo de apresentação de credenciais, e sua comunicação com outras entidades é feita com auxílio do protocolo HTTP, que encapsula mensagens XML.

7. CONSIDERAÇÕES FINAIS

Este capítulo, além de apresentar os pontos resultantes da comparação do modelo proposto com o PERMIS, formula as conclusões e, por fim, apresenta os direcionamentos que podem motivar trabalhos futuros.

7.1. COMPARAÇÕES COM O PERMIS

Ao comparar-se o modelo proposto com o PERMIS, algumas observações importantes podem ser notadas no referente aos seguintes fatores:

- autenticação;
- modelo de controle de acesso;
- distribuição de credenciais;
- delegação de privilégios;
- política de autorização;
- interface de programação.

7.1.1. Autenticação

Uma das principais características do PERMIS é o fato de ser indiferente à autenticação, ou seja, a tarefa de autenticar as entidades é deixada a cargo das aplicações que,

com isso, podem escolher que tipo de mecanismo utilizar. Em relação à autenticação, o objetivo do modelo proposto é utilizar um único mecanismo: os certificados de chave pública X.509 pertencentes à infra-estrutura ICP.

7.1.2. Modelo de controle de acesso

O modelo de controle de acesso adotado pelo modelo proposto é, de forma similar ao observado no PERMIS, o CABP. Assim, utilizando o conceito de papéis, os privilégios associam-se às entidades de forma indireta, o que propicia, entre outras coisas, maior flexibilidade e menor custo administrativo.

7.1.3. Distribuição de credenciais

A principal forma de distribuição de credencias adotada pelo PERMIS é o modelo de obtenção, no qual as informações necessárias para as decisões de acesso são obtidas de um repositório central. No modelo proposto, a escolha da forma de distribuição de credenciais fica a cargo da entidade que gerencia o domínio. A postura do modelo proposto é de que não há modelos de distribuição de credenciais melhores, apenas modelos mais adequados para uma determinada situação.

7.1.4. Delegação de privilégios

No PERMIS, não há mecanismos de suporte à delegação dinâmica de privilégios entre entidades finais. Isso significa que não há meios para que uma entidade final atribua privilégios a outras entidades finais de forma dinâmica sem a anuência de uma terceira parte. No modelo proposto, essa facilidade é alcançada através dos AGCAs, que interagem entre si com o auxílio do protocolo PDP.

7.1.5. Política de autorização

A política de autorização do PERMIS suporta a construção de validações que envolvem operações lógicas. Dessa forma, o tratamento da autorização combina uma série de variáveis. Inicialmente, a política de autorização adotada pelo modelo proposto não suporta esse tipo de funcionalidade.

7.1.6. Interface de programação

A utilização da infra-estrutura PERMIS está diretamente relacionada à sua interface de programação. Isso significa que uma aplicação que tenha por objetivo utilizar os serviços de autorização oferecidos pelo PERMIS deve invocar as funções contidas nessa interface de programação. O modelo proposto, ao invés de incentivar a construção (ou modificação) de aplicações que façam uso de funcionalidades de autorização através de uma interface de programação, proporciona autenticação e autorização sem que sejam necessárias

modificações nas aplicações existentes.

7.2. CONCLUSÃO

O modelo proposto mostra-se adequado para ambientes que tenham por meta controlar o acesso a recursos de rede. Através dele, é possível proporcionar às aplicações que lidam com informações sensíveis um modelo de controle de acesso que baseia seu funcionamento na interação entre as infra-estruturas X.509 ICP e IGP. Em um único modelo, é possível tratar a autenticação, a autorização e conseqüente controle de acesso, sem que haja a necessidade de se modificarem as aplicações existentes. Entretanto, devido ao fato de suportar um único mecanismo de autenticação, o modelo proposto tem sua flexibilidade reduzida. Nem todas as aplicações de rede suportam a premissa do modelo proposto que diz que os protocolos de acesso devem suportar o serviço de procuração das sessões de comunicação e o estabelecimento de canais de comunicação seguros com autenticação dupla.

Além disso, foi observado que a delegação dinâmica de privilégios entre entidades finais é uma facilidade que, embora factível, requer que algumas premissas sejam levadas em consideração: a delegação de privilégios entre entidades finais envolve operações, como a emissão de certificados, que devem ser realizadas apenas no âmbito da entidade final; em adição, uma das tarefas mais dispendiosas e mais complexas em ambientes que suportam a delegação, a validação dos caminhos de certificação envolvidos, só pode ser executada com eficiência quando o modelo de apresentação de credenciais for adotado.

Por fim, foi observado que, além da autenticação e da autorização, outros serviços de segurança podem ser adicionados à arquitetura do modelo proposto, tais como a auditoria e a tempestividade. Com isso, uma série de funcionalidades de segurança pode ser tratada em

uma única arquitetura.

7.3. TRABALHOS FUTUROS

Com o objetivo de estender a aplicabilidade do modelo proposto e aprimorar algumas das funcionalidades oferecidas, diversos temas para trabalhos futuros podem ser abordados.

7.3.1. Protocolos de acesso

Uma das restrições de implementação do modelo proposto está relacionada aos protocolos de acesso aos recursos suportados pela ECA. A estrutura de funcionamento da ECA pode ser modificada para suportar, além do HTTP, outros protocolos de acesso aos recursos protegidos. Opcionalmente, filtros que analisem as mensagens trocadas entre entidades finais e recursos protegidos podem ser acoplados à ECA. Esses filtros, em conjunto com mecanismos de detecção de intrusão (BACE; MELL, 2005) e de análise de comportamento, podem minimizar as tentativas de acesso inadvertido.

7.3.2. Política de autorização

Como melhoria, a exemplo do observado para o PERMIS, funcionalidades de suporte à construção de validações que utilizem operações lógicas podem ser acrescidas à PA. Dessa forma, situações de autorização mais complexas poderiam ser tratadas pela ECA. Por

exemplo: para acessar um recurso protegido, podem ser aplicadas restrições temporais nas quais, a cada período predeterminado, um conjunto diferente de privilégios seja necessário.

Além disso, a PA, ao invés de ser construída com base na política adotada pelo PERMIS, pode ser construída em conformidade com a linguagem *eXtensible Access Control Markup Language* (XACML). A linguagem XACML, encontrada em OASIS (2005), é uma das iniciativas abertas mais difundidas para a padronização de linguagens de descrição de políticas de autorização.

7.3.3. Determinação do contexto de acesso

Além das restrições de implementação referentes aos protocolos de acesso aos recursos protegidos, há uma outra restrição igualmente importante. Para que a determinação do contexto de acesso, no tocante ao recurso, não esteja restrita apenas aos endereços de rede, outras informações relacionadas ao recurso podem ser adicionadas à PA. A autorização e conseqüente controle de acesso podem ser tratados de forma granular se algumas outras características dos recursos, tais como o método sendo acesso, também forem levadas em consideração para determinação do contexto de acesso.

7.3.4. Hierarquia de delegação

Para que autorização e conseqüente controle de acesso aconteçam conforme as características do CABP, faz-se necessária a existência de dois certificados: o CEP, que especifica os privilégios associados a um determinado papel, e o CRP, que especifica a

associação entre uma entidade final e um conjunto de papéis. Geralmente, a responsabilidade pelo gerenciamento dos certificados CEP é assinalada a uma Autoridade de Atributos que, para atribuir privilégios às entidades finais (associações aos papéis), emite certificados CRP.

Em algumas situações, a emissão de um CRP pode envolver opções de delegação que habilitem a entidade final a agir como uma Autoridade de Atributos. Dessa forma, a entidade final também estaria apta a emitir certificados CEP, criando, assim, uma infra-estrutura onde a autoridade de emissão raiz seria a própria entidade final. Isso dá origem a uma hierarquia de delegação cuja característica principal é o encadeamento de infra-estruturas.

Para permitir esse tipo de facilidade, funcionalidades de gerenciamento de CEPs podem ser acrescidas ao agente AGCA.

7.3.5. Mobilidade

A estrutura da Lista de Credenciais e o funcionamento dos protocolos PSP e PDP podem ser alterados para que haja suporte à mobilidade. Com isso, uma entidade final poderia utilizar suas credenciais em múltiplas estações de trabalho desde que essas possuam o agente AGCA.

7.3.6. Auditoria

Visto que a análise de registros de eventos é um dos procedimentos de maior importância quando a auditoria de um ambiente computacional se faz necessária, manter registros íntegros e acurados das atividades de autorização e controle de acesso que tomaram

parte é um requisito fundamental. Para isso, ao modelo proposto pode ser adicionado um serviço de auditoria e manutenção segura de registros que faça uso, por exemplo, das técnicas observadas em Schneier e Kelsey (1998) e Chong, Peng e Hartel (2003).

7.3.7. Tempestividade

Algumas vezes, durante as atividades de auditoria, reconstruir a ordem de acontecimento dos eventos em um ambiente é um requisito de segurança fundamental. Dessa forma, manter o momento acurado em que uma requisição de acesso tomou parte é atividade de grande importância. Para situações como essa, uma fonte segura de tempo pode ser adicionada à arquitetura básica do modelo proposto.

7.3.8. Modelos de controle de acesso

Algumas situações de exceção requerem que a associação entre entidades finais e privilégios, feita pelo CABP de forma indireta, seja feita de forma discreta. Com isso, o modelo proposto pode ser modificado para que também haja suporte ao CAD.

7.3.9. Desempenho

Quando o desempenho e a disponibilidade forem fatores determinantes, é possível que, dentro de um mesmo domínio, exista uma ou mais ECAs.

REFERÊNCIAS BIBLIOGRÁFICAS

ADAMS, C.; FARRELL, S.; KAUSE, T.; MONONEN, T. RFC 4210 - Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), 2005. Disponível em: <http://www.ietf.org/rfc/rfc4210.txt>. Acesso em: 12 dez. 2005.

ARSENAULT, A.; TURNER, S. Internet X.509 Public Key Infrastructure: Roadmap, 2002. Disponível em: <http://tools.ietf.org/wg/pkix/draft-ietf-pkix-roadmap/draft-ietf-pkix-roadmap-09.txt>. Acesso em: 17 dez. 2005.

BACE, R.; MELL, P. Intrusion Detection Systems. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>. Acesso em: 17 jul. 2005.

BECKER, M. Y. Cassandra: flexible trust management and its application to electronic health records. Disponível em: <http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-648.pdf>. Acesso em: 16 dez. 2005.

BELL, D.; LAPADULA, L. **Secure Computer Systems: Mathematical Foundations and Model**. Estados Unidos: The Mitre Corporation, 1973. 134 p.

BENJUMEA, B.; LOPEZ, J.; MONTENEGRO, J. A.; TROYA, J. M. A First Approach to Provide Anonymity in Attribute Certificates. In: Public Key Cryptography - International Workshop on Theory and Practice in Public Key Cryptography, 7, 2004, Cingapura. **Proceedings...** Estados Unidos: Springer, 2004, p. 402-415.

BERTINO, E.; BETTINI, C.; FERRARI, E.; SAMARATI, P. An Access Control Model Supporting Periodicity Constraints and Temporal Reasoning. **ACM Transactions on Database Systems**, Estados Unidos, v. 23, p. 231-285, set. 1998.

BIBA, K. J. **Integrity considerations for secure computer systems**. Estados Unidos: The Mitre Corporation, 1977. 125 p.

BINDER, J. C. Introduction to PKI - Public Key Infrastructure. Disponível em: <http://www.k-binder.be/Papers/PKI_V11.pdf>. Acesso em: 10 nov. 2004.

BLAZE, M.; FEIGENBAUM, J.; IOANNIDIS, J. RFC 2704 - The KeyNote Trust-Management System, 1999. Disponível em: <http://www.ietf.org/rfc/rfc2704.txt>. Acesso em: 14 jul. 2003.

BLOBEL, B.; HOEPNER, P.; JOOP, R.; KARNOUSKOS, S.; KLEINHUIS, G.; STASSINOPOULOS, G. Using a privilege management infrastructure for secure web-based ehealth applications. **Computer Communications**, Estados Unidos, v. 26, p. 1863-1872, out. 2003.

BURNETT, S.; PAINE, S. **RSA security's official guide to cryptography**. EstadosUnidos: McGraw-Hill Osborne Media, 2001. 419 p.

BURR, W.; DODSON, D.; NAZARO, N.; POLK, W. T. MISPC Minimum Interoperability Specification for PKI Components. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-15/SP800-15.pdf>. Acesso em: 21 ago. 2004.

BURRUSS, J. R. ROAM - An Authorization Manager for Grids. Disponível em: <http://web.gat.com/~burruss/burruss-jgc-2005-draft-v1.pdf>. Acesso em: 2 dez. 2005.

CANTOR, S.; ERDOS, N. Shibboleth-architecture draft v05. Disponível em: <http://shibboleth.internet2.edu/draft-internet2-shibboleth-arch-v05.html>. Acesso em: 12 dez. 2005.

CHADWICK, D. W.; OTENKO, A. The PERMIS X.509 Role Based Privilege Management Infrastructure. In: ACM Symposium on Access Control Models and Technologies (SACMAT), 7, 2002, Estados Unidos. **Proceedings…** Estados Unidos: ACM Press, 2002. p. 135-140.

CHADWICK, D. W.; OTENKO, A. RBAC Policies in XML for X.509 Based Privilege Management. In: International Conference on Information Security, 17, 2002, Egito. **Proceedings...** Holanda: Kluwer Academic Publishers, 2002. p. 39-53.

CHADWICK, D. W.; OTENKO, A. A Comparison of the Akenti and PERMIS Authorization Infrastructures. In: ITI International Conference on Information and Communications Technology, 1, 2003, Egito. **Proceedings...** Holanda: Kluwer Academic Publishers, 2003. p. 5-26.

CHADWICK, D. W.; OTENKO, A.; BALL, E. Role-based access controls with X.509 attribute certificates. **IEEE Internet Computing**, Estados Unidos, v.7, p. 62-69, abr. 2003.

CHANG-JI, W.; JIAN-PING, W.; HAI-XIN, D. Using attribute certificate to design role-based access control. In: International Conference on Parallel and Distributed Computing, Applications and Technologies, 4, 2003, Estados Unidos. **Proceedings...** Estados Unidos: IEEE Press, 2003. p. 216-218.

CHONG, C. N.; PENG, Z.; HARTEL, P. H. Secure audit logging with tamper-resistant hardware. In: International Conference on Information Security, Security and Privacy in the Age of Uncertainty, 18, Grécia. **Proceedings...** Estados Unidos: Kluwer Academic Publishers, 2003. p. 73-84.

CRAMPTON, J.; KHAMBHAMMETTU, H. Authorization and certificates: Are we pushing when we should be pulling?. In: IASTED International Conference on Communication, Network, and Information Security, 2003, Estados Unidos. **Proceedings..**. Estados Unidos: ACTA Press, p. 62-66, 2003.

DAMIANOU, H.; DULAY, N.; LUPU, E.; SLOMAN, M. The Ponder Policy Specification Language. In: Workshop on Policies for Distributed Systems and Networks, 2001, Inglaterra. **Proceedings...** Alemanha: Springer, 2001. p. 18-39.

DAWSON, E.; LOPEZ, J.; MONTENEGRO, A.; OKAMOTO, E. A new design of privilege management infrastructure for organizations using outsourced PKI. In: International Conference on Information Security, 5, 2002, Brasil. **Proceedings...** Alemanha: Springer, 2002. p. 136-149.

DEPARTMENT OF DEFENSE. Department of Defense Trusted Computer Evaluation Criteria, 1985. Disponível em: <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html>. Acesso em: 4 jul. 2005.

DIERKS, T.; ALLEN, C. RFC 2246 - The TLS Protocol Version 1.0, 1999. Disponível em: <http://www.ietf.org/rfc/rfc2246.txt>. Acesso em: 23 abr. 2004.

EVERED, M.; BÖGEHOLZ, S. A Case Study in Access Control Requirements for a Health Information System. In: Workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation, 2004, Nova Zelândia. **Proceedings...** Austrália: Australian Computer Society, 2004, p. 53-61.

FAGIN, R.; On an authorization mechanism. **ACM Transactions on Database Systems**, v. 1, Estados Unidos, p. 310-319, 1978.

FARRELL, S.; HOUSLEY, R. RFC3281 - An Internet Attribute Certificate Profile for Authorization, 2002. Disponível em: <http://www.ietf.org/rfc/rfc3281.txt>. Acesso em: 4 jan. 2004.

FERNANDEZ, R. Enterprise Dynamic Access Control (EDAC) - Case Study. Disponível em: <http://csrc.nist.gov/rbac/EDACcase-study.doc>. Acesso em: 14 nov. 2005.

FERRAIOLO, D. F.; KUHN, D. R. Role Based Access Control. In: NIST-NSA National Computer Security Conference, 15, 1992, Estados Unidos. **Proceedings…** Estados Unidos: NIST, 1992, p. 554-563.

FIELDING, R.; GETTYS, J.; MOGUL, J.; FRYSTYK, H.; MASINTER, L.; LEACH, P.; BERNERS-LEE, T. RFC 2616 - Hypertext Transfer Protocol - HTTP/1.1, 1999. Disponível em: <http://www.ietf.org/rfc/rfc2616.txt>. Acesso em: 13 jan. 2005.

FREED, N.; BORENSTEIN, N. RFC 2045 - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, 1996. Disponível em: <http://www.ietf.org/rfc/rfc2045.txt>. Acesso em: 19 abr. 2004.

FREIER, A. O.; KARLTON, P.; KOCHER, P. C. The SSL Protocol Version 3.0, 1996. Disponível em: <http://wp.netscape.com/eng/ssl3/draft302.txt>. Acesso em: 17 abr. 2004.

GRIFFITHS, P. P.; WADE, B. W. An authorization mechanism for a relational database system. **ACM Transactions on Database Systems**, Estados Unidos, v. 1, p. 242-255, 1976.

HOUSLEY, R.; POLK, W.; FORD, W.; SOLO, D. RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2002. Disponível em: <http://www.ietf.org/rfc/rfc3280.txt>. Acesso em: 4 jan. 2004.

IAIK CRYPTO TOOLKITS. Disponível em: <http://jce.iaik.tugraz.at/sic/products/core_crypto_toolkits>. Acesso em: 3 set. 2005.

ITU-T Recommendation X.500, Information Technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services, 2001.

ITU-T Recommendation X.509, Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, 2000.

ITU-T Recommendation X.812, Information technology - Open Systems Interconnection - Security Frameworks for open systems: Access control framework, 1995.

JAVA SERVLET TECHNOLOGY. Disponível em: <http://java.sun.com/products/servlet/>. Acesso em: 16 jun. 2005.

JOHNSTON, W.; MUDUMBAI, S.; THOMPSON, M. Authorization and attribute certificates for widely distributed access control. In: IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 7, 1998, Estados Unidos. **Proceedings…** Estados Unidos: IEEE Computer Society, 1998, p. 340–345.

JOSHI, J. B. D.; BERTINO, E.; LATIF, U.; GHAFOOR, A. A Generalized Temporal Role-Based Access Control Model, **IEEE Transactions on Knowledge and Data Engineering**, Estados Unidos, v. 17, p. 4-23, jan. 2005.

KNIGHT, G. S.; GRANDY, C. Scalability Issues in PMI Delegation. In: Annual PKI Research Workshop, 1, 2002, Estados Unidos. **Proceedings...** Estados Unidos: NIST, 2002, p. 77-87.

LAMPSON, B. Protection. In: Princeton Conference on Information Sciences and Systems, 5, 1971, Estados Unidos. **Proceedings...** Estados Unidos: ACM Press, 1974, p. 18-24.

LINN, J. RFC 1421 - Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures, 1993. Disponível em: <http://www.ietf.org/rfc/rfc1421.txt>. Acesso em: 19 abr. 2004.

MEINEL, C.; ZHOU, W. Implement role based access control with attribute certificates. In: Conference of Advanced communication Technology, 6, 2004, Coréia. **Proceedings…** Estados Unidos: IEEE Computer Society, 2004. p, 536-541.

MENEZES, A. J.; OORSCHOT, P. V.; VANSTONE, S. A. Handbook of Applied Cryptography. Estados Unidos: CRC Press, 1996. 816 p.

MICROSOFT SQL SERVER. Disponível em: <http://www.microsoft.com/sql/default.mspx>. Acesso em: 9 nov. 2005.

MILLS, D. L. The Network Time Protocol Version 4 Protocol Specification, 2005. Disponível em: <http://www.ietf.org/internet-drafts/draft-ietf-ntp-ntpv4-proto-01.txt>. Acesso em: 3 dez. 2005.

MOTTA, G. H. M. B. **Um modelo de autorização contextual para o controle de acesso ao prontuário eletrônico do paciente em ambientes abertos e distribuídos**. 2003. 212 f. Tese (Doutorado em Engenharia Elétrica) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2003.

MYERS, M.; ANKNEY, R.; MALPANI, A.; GALPERIN, S.; ADAMS, C. RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP), 1999. Disponível em: <http://www.ietf.org/rfc/rfc2560.txt>. Acesso em: 12 out. 2004.

NATIONAL COMPUTER SECURITY CENTER. A Guide To Understanding Discretionary Access Control In Trusted Systems. Disponível em: <http://www.fas.org/irp/nsa/rainbow/tg003.htm>. Acesso em: 08 set. 2003.

NOCHTA, Z.; EBINGER, P.; ABECK, S. PAMINA: A Certificate Based Privilege Management System. In: Network and Distributed System Security Symposium, 2002, Estados Unidos. **Proceedings...** Estados Unidos: The Internet Society, 2002.

OASIS. eXtensible Access Control Markup Language (XACML) version 1.0. Disponível em: <http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf>. Acesso em: 13 ago. 2005.

PERMIS. Privilege and Role Management Infrastructure Standards Validation. Disponível em: <http://sec.isi.salford.ac.uk/permis/>. Acesso em: 05 fev. 2004.

POLEMI, D.; HOEPNER, P.; BOURKA, A. HARP - Harmonisation for the Security of Web Technologies and Applications. Disponível em: <http://www.telecom.ntua.gr/~HARP/HARP/INSIDE/PublicDel/HARPWP2D22v09.zip>. Acesso em: 29 jul. 2002.

PRIME Consortium. PRIME White Paper. Disponível em: <http://www.prime-project.eu.org/whitepaper/prime/public/press_room/whitepaper/PRIME-Whitepaper-V1.pdf>. Acesso em: 15 dez. 2005.

RESCORLA, E. RFC 2818 - HTTP Over TLS, 2000. Disponível em: <http://www.ietf.org/rfc/rfc2818.txt>. Acesso em: 25 jun. 2004.

SALTZER, J. H.; SCHROEDER, M. D. The protection of information in computer systems. Disponível em: <http://www.cap-lore.com/CapTheory/ProtInf/>. Acesso em: 5 nov. 2005.

SANDHU, R. S. Lattice-based access control models. **IEEE Computer**, Estados Unidos, v. 26, p. 9-19, 1993.

SANDHU, R. S.; SAMARATI, P. Access control: Principles and Practice. **IEEE Communications**, Estados Unidos, v. 32, p. 40-48, 1994.

SANTESSON, S.; HOUSLEY, R.; FREEMAN, T. RFC 3709 - Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates, 2004. Disponível em: <http://www.ietf.org/rfc/rfc3709.txt>. Acesso em: 2 out. 2004.

SCHNEIER, B.; KELSEY, J. Cryptographic Support for Secure Logs on Untrusted Machines, USENIX Security Symposium, 7, Estados Unidos. **Proceedings...** Estados Unidos: USENIX Press, 1998. p. 53-62.

SEIGNEUR, J. M.; FARRELL, S.; JENSEN, C. D.; GRAY, E.; CHEN, Y. End-to-end Trust Starts with Recognition. In: International Conference on Security in Pervasive Computing, 1, 2003, Alemanha. **Proceedings...** Alemanha: Springer, 2004. p. 130-142.

SEITZ, L.; PIERSON, J. M.; BRUNIE, L. **Sygn: A certificate based access control in Grid environments**. França: Laboratoire d'InfoRmatique en Images et Systèmes d'informatio (Liris), 2005. 15 p.

SHIREY, R. RFC 2828 - Internet Security Glossary, 2000. Disponível em: <http://www.ietf.org/rfc/rfc2828.txt>. Acesso em: 2 fev. 2004.

SOUZA, J. N.; CUNHA, C. C.; VILLAR, M.; DINIZ, A. L. Segurança nos Processos de Autenticação e Autorização Através de Certificados X.509. In: Simpósio Segurança em Informática - SSI 2004, 6, 2004, Brasil. **Anais...** Brasil: Biblioteca Central do ITA/CTA, 2004.

THE OPEN GROUP. Authorization (AZN) API. Inglaterra: The Open Group, 2000. p. 110.

VOLLBRECHT, J.; CALHOUN, P.; FARRELL, S.; GOMMANS, L.; GROSS, G.; BRUIJN, B.; LAAT, C.; HOLDREGE, N.; SPENCE, D. RFC 2904 - AAA Authorization Framework, 2000. Disponível em: <http://www.ietf.org/rfc/rfc2904.txt>. Acesso em: 25 ago. 2005.

WOHLMACHER, P; PHAROW, P. Applications in Health Care using Public-Key Certificates and Attribute Certificates. In: Annual Computer Security Applications Conference, 16, 2000, Estados Unidos. **Proceedings...** Estados Unidos: IEEE Computer Society, 2000, p. 128-137.

XERCES PROJECT. Disponível em: <http://xerces.apache.org/>. Acesso em: 14 ago. 2005.

YEONG, W.; HOWES, T.; KILLE, S. RFC 1777 – Lightweight Directory Access Protocol, 1995. Disponível em: <http://www.ietf.org/rfc/rfc1777.txt>. Acesso em: 2 jul. 2004.

APÊNDICE A – CRIPTOGRAFIA

Através da criptografia, alguns objetivos da segurança da informação, como o sigilo, a integridade e a autenticação, podem ser endereçados de forma adequada. Isso faz com que uma das mais importantes aplicações da criptografia esteja relacionada à prevenção e detecção de atividades maliciosas. Para isso, a criptografia utiliza-se de mecanismos simétricos, assimétricos e de algumas funções especiais, como, por exemplo, as funções de resumo.

1. CRIPTOGRAFIA SIMÉTRICA

Nessa modalidade de criptografia, também conhecida por criptografia de chave de sessão, ou ainda criptografia de chave secreta, as operações criptográficas se fazem por meio de uma única chave compartilhada entre os extremos da comunicação.

Significativamente mais rápidos quando comparados à criptografia assimétrica, os algoritmos que praticam a criptografia simétrica são amplamente utilizados para cifrar grandes quantidades de dados. Porém, essa rapidez tem um preço: a segurança. Qualquer entidade que tiver em mãos a chave de sessão poderá decifrar a informação mesmo que esta não possua autorização para tal.

O cenário geral de utilização da criptografia de chave simétrica pode ser observado na Figura 38, na qual duas entidades, origem e destino, fazem parte de um esquema de comunicação no qual E_e e D_d representam, respectivamente, as funções responsáveis pelas operações de criptografia e decriptografia. Com o intuito de transmitir uma mensagem m, a

origem determina e, uma chave escolhida aleatoriamente dentro de um espaço de chaves. Tem-se então que a mensagem cifrada c a ser enviada ao destino é $E_e(m)=c$. Sendo assim, o destino só estará apto a decifrá-la se $D_d(c)=m$, sendo que a chave criptográfica d é determinada por $d=e^{-1}$.

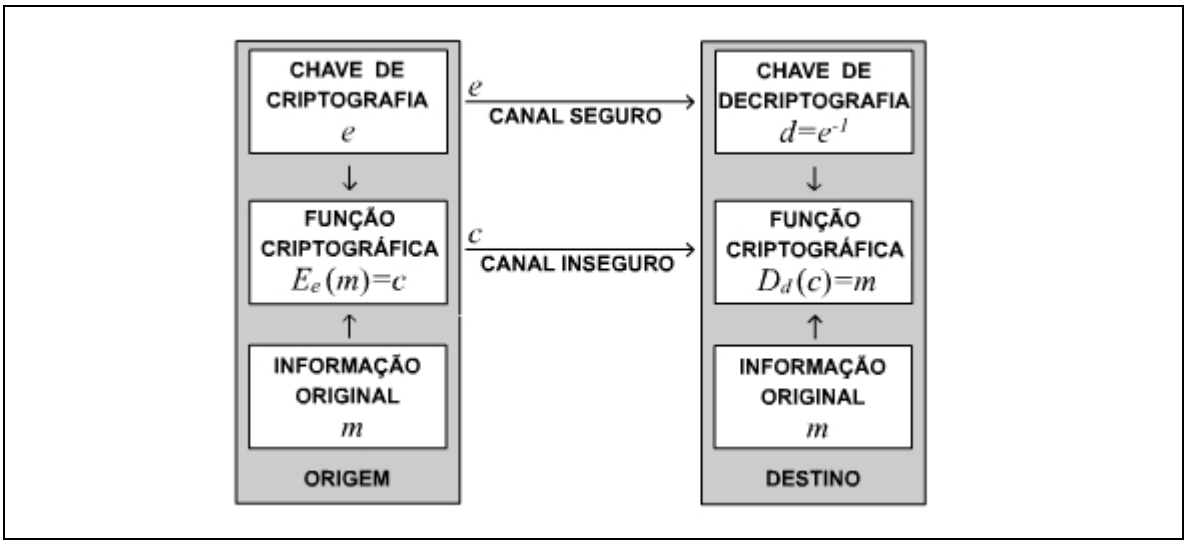

Figura 38. Criptografia simétrica.

Observa-se que a segurança do processo de comunicação está diretamente relacionada ao sigilo chave secreta e. É imprescindível que as entidades envolvidas mantenham a chave e em absoluto sigilo, longe de qualquer parte mal-intencionada. Para tal é necessário que exista um mecanismo seguro de compartilhamento de chaves, seja ele digital ou não. No entanto, qualquer que seja esse mecanismo, não tornará a distribuição das chaves em ampla escala uma atividade menos dispendiosa, já que para uma comunidade com total de n participantes, cada um de seus membros pode manter, potencialmente, a quantidade de $n-1$ chaves.

As questões relacionadas ao compartilhamento de chaves ou mesmo à sua distribuição em esquemas de ampla escala tiveram sua severidade amenizada com o advento da criptografia de chave pública. Nela, a transmissão das chaves utilizadas durante as operações

de geração de cifras é realizada por meio de técnicas de criptografia assimétrica. Nenhuma chave secreta é transmitida nem mesmo compartilhada.

2. CRIPTOGRAFIA ASSIMÉTRICA

Na criptografia assimétrica, também conhecida como criptografia de chave pública, cada entidade, ao invés de possuir uma única chave, como ocorre em esquemas baseados em criptografia simétrica, possui ao menos um par delas, definido por (e, d). A parte pública do par, representada por e, não deve ser mantida em segredo; ao contrário, deve ser amplamente distribuída. Já a parte privada, d, deve ser mantida em sigilo absoluto. Apenas seu criador deve ter a capacidade de utilizá-la.

O cenário de utilização da criptografia assimétrica, ilustrado na Figura 39, utiliza as mesmas definições feitas para os esquemas simétricos. Mas, dessa vez, a chave criptográfica e utilizada no processo de criptografia da mensagem não será gerada aleatoriamente na origem. Será utilizada, na verdade, a chave pública do destino. Dessa forma, apenas aquele que possuir a parte privada do par de chaves será capaz de decifrar a mensagem.

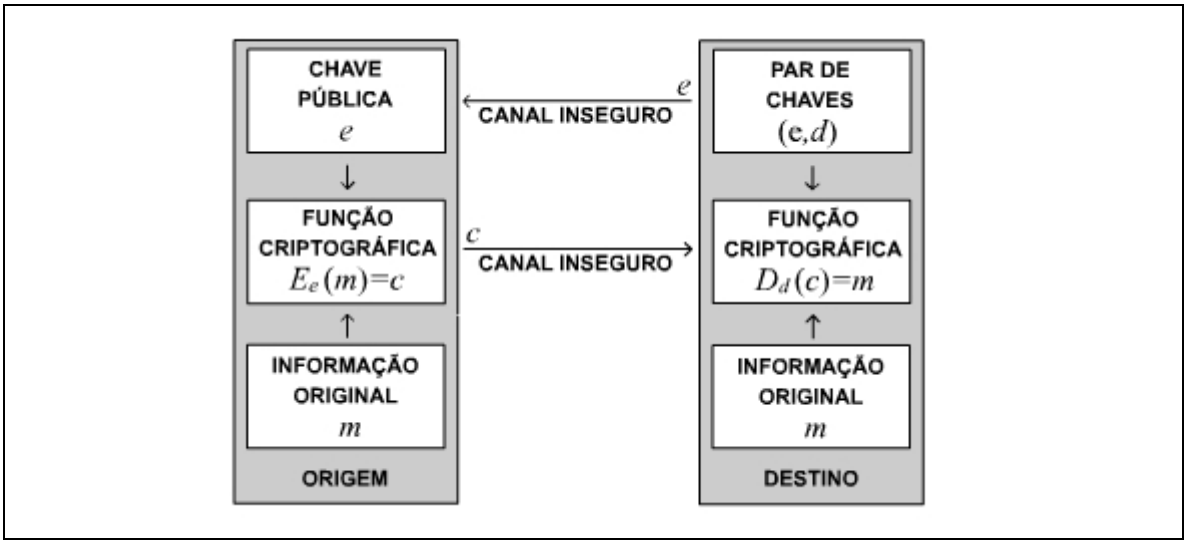

Figura 39. Criptografia assimétrica.

Em esquemas criptográficos como esse é fundamental ter convicção de que a chave e utilizada pela origem para geração da mensagem cifrada c forma o par pertencente ao destino. Para tal, a criptografia de chave pública deve utilizar-se de outras técnicas criptográficas: as assinaturas digitais. Através dessa aliança caracteriza-se outro grande benefício da modalidade de criptografia assimétrica: a autenticação. Entretanto, a assinatura digital obtida com o uso da criptografia assimétrica, por se tratar de um processo extremamente dispendioso, não pode ser utilizada de forma isolada. É necessária a existência de um mecanismo capaz de proporcionar integridade dos dados, denominado função de resumo (*hash*).

3. FUNÇÕES DE RESUMO

Funções de resumo que, conforme dito anteriormente, são utilizadas em conjunção com assinaturas digitais a fim de garantir a integridade dos dados, transformam mensagens de tamanho variável em uma seqüência de tamanho fixo de caracteres aleatórios. Indo de

encontro à necessidade de um mecanismo que proporcione maior agilidade ao moroso processo de geração de assinaturas assimétricas, essa capacidade de compressão, faz com que o uso de funções de resumo seja amplamente difundido.

4. ASSINATURAS DIGITAIS

Essenciais para autenticação, autorização e não-repúdio, as assinaturas digitais têm como objetivo principal prover meios a uma entidade para que esta possa relacionar sua identidade a um pedaço de informação. Esses meios, traduzidos em dois processos – geração e verificação de assinaturas –, geralmente baseiam seu funcionamento na utilização de técnicas de criptografia assimétrica aliadas às funções de resumo.

No esquema criptográfico ilustrado na Figura 40, a entidade emissora deseja proporcionar meios para que o destino verifique a autenticidade da mensagem transmitida. A origem, com o intuito de gerar uma assinatura digital de uma mensagem m, determina s, conseqüência da aplicação de uma operação de criptografia E_d usando a chave privada e sobre o resultado de uma função de resumo H. Sendo assim, temos que $E_d(H(m)) = s$.

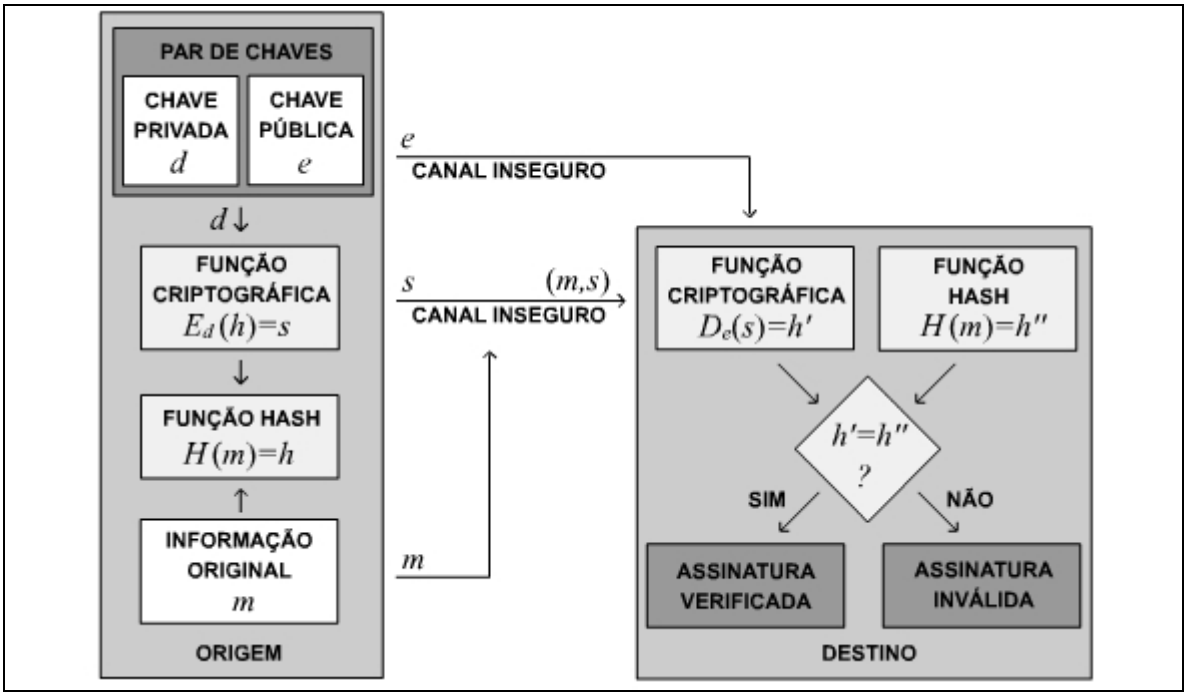

Figura 40. Assinatura digital.

Ao destino é então transmitido o par (m,s) e, para que a autenticidade dessa assinatura possa ser verificada, o destino deve determinar se é verdadeira a seguinte equação: $D_e(s) = H(m)$, na qual D_e representa uma função de decriptografia do sistema que utiliza a chave pública da origem para decifrar as mensagens.

A assinatura digital, portanto, é o elemento responsável por prover meios que assegurem a relação entre uma entidade digital e pedaços de informação. Ao permitir que uma entidade não possa repudiar a ocorrência de um evento, a assinatura digital se torna uma das técnicas mais utilizadas quando o assunto é prevenir fraudes eletrônicas.