Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Celso Fukushima

Aplicabilidade de Certificados de Atributos no Âmbito da ICP-Brasil

São Paulo

2010

Celso Fukushima

Aplicabilidade de Certificados de Atributo no Âmbito da ICP-Brasil

Dissertação de Mestrado apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, como parte dos requisitos para a obtenção do título de Mestre em Engenharia de Computação.

Área de Concentração: Rede de Computadores

Data da aprovação ____/____/____

_____

Prof. Dr. Volnys Borges Bernal (Orientador)

IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Membros da Banca Examinadora:

Prof. Dr. Volnys Borges Bernal (Orientador)

IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Prof. Dr. Adilson Eduardo Guelfi (Membro)

IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Prof. Dr Edson Midorikawa (Membro)

USP – Universidade de São Paulo

Celso Fukushima

Aplicabilidade de Certificados de Atributo no Âmbito da ICP-Brasil

Dissertação de Mestrado apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, como parte dos requisitos para a obtenção do título de Mestre em Engenharia de Computação.

Área de Concentração: Rede de Computadores

Orientador: Prof. Dr. Volnys Borges Bernal

São Paulo

Julho/2010

DEDICATÓRIA

Dedico este trabalho ao meu pai, Kiyoshi Fukushima,

que me ensinou a lutar

à minha mulher Andréa e à pequena Natália,

que são a razão da minha luta.

“Escolhe um trabalho de que gostes, e não terás que trabalhar nem um dia na tua vida.”

Confúcio

AGRADECIMENTOS

À minha filha Natália, por existir.

À minha mulher Andréa, pelo seu amor e compreensão nos momentos em que estive ausente por causa deste trabalho.

Ao meu pai Kiyoshi, que sempre me apoio em todas as minhas iniciativas.

Aos meus irmãos, Miriam, Eli, Lígia e Thiago e à minha madrasta Lúcia que sempre acreditaram na minha capacidade.

À minha mãe Satiko (*in memorian*) que sempre está comigo.

Ao meu orientador Prof. Dr. Volnys Borges Bernal, pelo seu conhecimento, paciência, dedicação e por me motivar a concluir este trabalho.

À banca examinadora pelas sugestões construtivas que se delinearam durante a qualificação e defesa desta dissertação.

Ao Dr. Alexandre Wald e ao Prof. Arnoldo Wald, por acreditarem no meu projeto.

RESUMO

Cada vez mais os certificados digitais fazem parte do nosso cotidiano, pois os benefícios desta tecnologia são evidentes no mundo digital atual. A cada momento, mais e mais pessoas e empresas têm adotado os certificados digitais nas suas transações eletrônicas. Entretanto, existem problemas no atual perfil de certificado digital adotado pelo Brasil (ICP-Brasil), entre eles: (a) a centralização em um mesmo certificado de funções de autenticação e de qualificação; (b) a diferença dos prazos de validade entre os certificados de identidade e os diversos atributos (do portador) nele contidos e (c) a inclusão de atributos provenientes de diferentes fontes de autoridade em um mesmo certificado de identidade. Soma-se a isso, a falta de conhecimento do mercado sobre a tecnologia dos Certificados de Atributos (CA), que é um tipo de certificado criado especificamente para designar qualidades ao portador. Por estes motivos algumas entidades têm adotados certificados de chaves públicas, não apenas para realizar a identificação, mas também prover qualificações às pessoas, com o intuito de determinar as suas permissões de acesso. A utilização de certificados digitais de identidade com atributos causam os seguintes impactos: (a) a complexidade do estabelecimento e operação de uma fonte de autoridade que neste modelo é baseado em Infraestrutura de Chave Pública (ICP); (b) a revogação de um certificado de identidade não deveria afetar a revogação de seus atributos e vice-versa, ou seja, a revogação de um atributo não deveria revogar o certificado de identidade; (c) a inserção de vários atributos em um mesmo certificado cria um vínculo desnecessário entre atributos totalmente distintos, uma vez que eles geralmente são de diferentes fontes de autoridade com variados prazos de validade; e (d) os CAs são alternativas viáveis para serem usados nos processos de qualificação das entidades, pois são seguros, simples de serem administrados, legais do ponto de vista jurídico e interoperáveis entre sistemas heterogêneos. Esta dissertação realiza uma análise da aplicabilidade dos certificados de atributos em operação conjunta com certificados emitidos no âmbito da ICP-Brasil, mostrando as alternativas práticas de modelos de infraestrutura de certificados baseados em CA, analisando comparativamente os benefícios que esta tecnologia traz para as operações do cotidiano das pessoas e empresas, atendendo os requisitos de segurança no processo de identificação e atribuição de privilégios dos usuários.

Palavras-chave: certificado de atributo; infraestrutura de chaves públicas; ICP; infraestrutura de gerenciamento de privilégios; IGP; ICP-Brasil.

ABSTRACT

Applicability of attributes certificates in the scope of PKI-Brazil (ICP-Brasil)

Increasingly, the digital certificates are part of our daily lives, because the benefits of this technology are evident in the digital world today. More and more people and businesses have adopted the digital certificates in their electronic transactions. However, problems exist in the current model of the digital certificate used by Brazil (ICP-Brazil), including: (a) centralization in a single certificate of authentication and qualifications functions, (b) differences between the periods of validity certificates of identity and the different owner's attributes it contains: and (c) the inclusion of attributes from different sources of authority in the same certificate of identity. Furthermore the lack of market knowledge about the technology of Attribute Certificates, which is a type of certificate created specifically to describe the qualities of the owner aggravates the problem. For these some entities have adopted certificates based on Public Key Infrastructure (PKI), not only to perform the identification, but also to provide people's qualification in order to determine their access permissions. The use of digital certificates based on PKI with attributes cause the following impacts: (a) the high complexity of establishing and operating a PKI, (b) the revocation of a PKI certificate, should not affect the repeal of its attributes and vice versa, which means, the withdrawal of an attribute should not revoke the PKI certificate, (c) the insertion of several attributes in the same certificate creates an unnecessary link between completely different attributes, since they are usually from different sources of authority with several validity periods, and (d) the Attribute Certificates (AC) are feasible alternatives to be used in the process of qualification of entities, because they are safe, simple to be managed, meet the legal requirements and they are interoperable across heterogeneous systems. This dissertation performs an analysis of the applicability of Attributes Certificates in a joint operation with public key certificates issued under the ICP-Brazil, showing practical alternative models of infrastructure based on AC, comparatively analyzing the benefits that technology brings to the operations of the daily lives of people and companies, given the security requirements in the identification and assignment of user privileges.

Key-Words: attribute certificate; public key infrastructure; PKI; privileges management infrastructure; PMI; ICP-Brasil.

Lista de Ilustrações

Lista de Tabelas

Lista de abreviaturas

AA	Autoridade de Atributo
AASP	Associação dos Advogados de São Paulo
AC	Autoridade Certificadora
ACL	*Access Control List*
ADF	*Access Control Decision Function*
AEF	*Access Control Enforcemente Function*
ANS	Agência Nacional de Saúde Suplementar
API	*Application Programming Interface*
AR	Autoridade de Registro
ASN1	*Abstract Syntax Notation One*
AUTELSI	*Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información*
AZN	*Authorization*
BSI	*British Standards Institution*
CA	Certificado de Atributo
CAD	Certificado de Atributo de Delegação
CAP	Certificado de Atributo de Política
CERES	*Autoridad Pública de Certificación Española*
CFE	Conselho Federal de Enfermagem
CFM	Conselho Federal de Medicina
CI	Certificado de Identidade (de chave pública)
CNES	Cadastro Nacional de Estabelecimentos de Saúde
CREMESP	Conselho Regional de Medicina do Estado de São Paulo
DAC	*Discretionary Access Control*

DNIS	*Databases in Networked Information Systems*
DTD	*Document Type Definition*
ETSI	*European Telecommunications Standards Institute*
FAA	Fonte de Autoridade de Atributo
FNMT	*Fábrica Nacional de Moneda y Timbre*
ICAM	*Ilustre Colégio de Abogados de Madrid*
ICP	Infraestrutura de Chaves Públicas
ICP-Brasil	Infraestrutura de Chaves Públicas do Brasil
IGP	Infraestrutura de Gerenciamento de Privilégios
IRPF	Imposto de Renda Pessoa Física
ISO	*International Organization for Standardization*
LCAR	Lista de Certificados de Atributos Revogados
LCR	Lista de Certificados Revogados
LDAP	*Lightweight Directory Access Protocol*
LNCS	*Lecture Notes in Computer Science*
OAB	Ordem dos Advogados do Brasil
OCSP	*Online Certificate Status Protocol*
PA	*Privilege Allocator*
PC	Política de Certificado
PERMIS	*PrivilEge and Role Management Infrastructure Standards validation*
PKI	*Public Key Infrastructure*
RBAC	*Role-based access control*
RFB	Receita Federal do Brasil
RFC	*Request for Comments*

RH	Recursos Humanos
RIC	Registro Único de Identidade Civil
SBC	Sociedade Brasileira de Cardiologia
SBRad	Sociedade Brasileira de Radiologia
Siscomex	Sistema Integrado de Comércio Exterior
S/MIME	*Secure/Multipurpose Internet Mail Extension*
SOA	*Source Of Authority*
S-RES	Sistema de Registro Eletrônico de Saúde
SSL	*Socket Secure Layer*
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
XML	*eXtensible Markup Language*

Sumário

1 INTRODUÇÃO

1.1 Motivação

O perfil de certificado digital adotado no âmbito da Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil) é um perfil chamado de centralizado (PERMIS, 2007), uma vez que concentra em um único certificado funções de identificação e qualificação do usuário. Os campos que identificam o usuário têm o objetivo de associar o titular ao certificado. Exemplos: nome e data de nascimento do usuário. Os campos que qualificam o usuário têm o objetivo de definir os privilégios que a pessoa tem para acessar determinados recursos. Exemplos: CPF e Título de Eleitor são informações que conferem qualificações ao portador: o de ser contribuinte da Receita Federal do Brasil (RFB) e o de ser eleitor cadastrado no Tribunal Regional Eleitoral (TRE), respectivamente.

Recentemente, em outubro de 2007, a Ordem dos Advogados do Brasil (OAB) se tornou uma Autoridade Certificadora (AC) de âmbito da ICP-Brasil (Figura 1) com o objetivo de emitir certificados digitais aos seus advogados associados. A opção da OAB de entrar na árvore de certificação da ICP-Brasil é um grande avanço para a disseminação dos certificados digitais. Entretanto, novamente o perfil adotado centraliza em um único certificado as funções de identificação e qualificação, uma vez que a AC-OAB só emite certificados de identidade (CI) para os seus advogados.

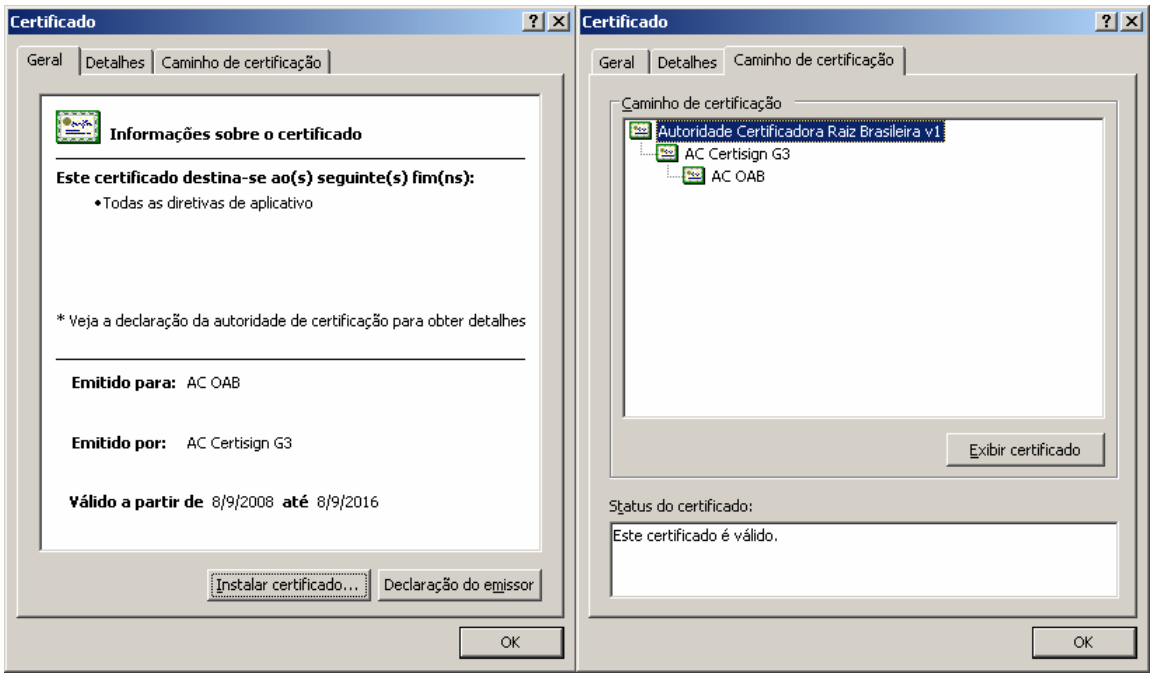

Figura 1 - Certificado da AC-OAB e o respectivo caminho de certificação

Fonte: elaborado pelo autor e obtido por meio do próprio certificado digital da AC OAB (2009)

Além da OAB, o Conselho Federal dos Contabilistas (CFC) firmou um acordo em setembro de 2007, com a Federação Nacional das Empresas de Serviços Contábeis e das Empresas de Assessoramento, Perícias, Informações e Pesquisas (FENACON) e, por meio de uma AC (AC Fenacon Certisign) no âmbito da ICP-Brasil, passou a fornecer os CIs aos seus contadores. Esta AC é uma subordinada à AC da Secretaria da Receita Federal (SRF) (Figura 2).

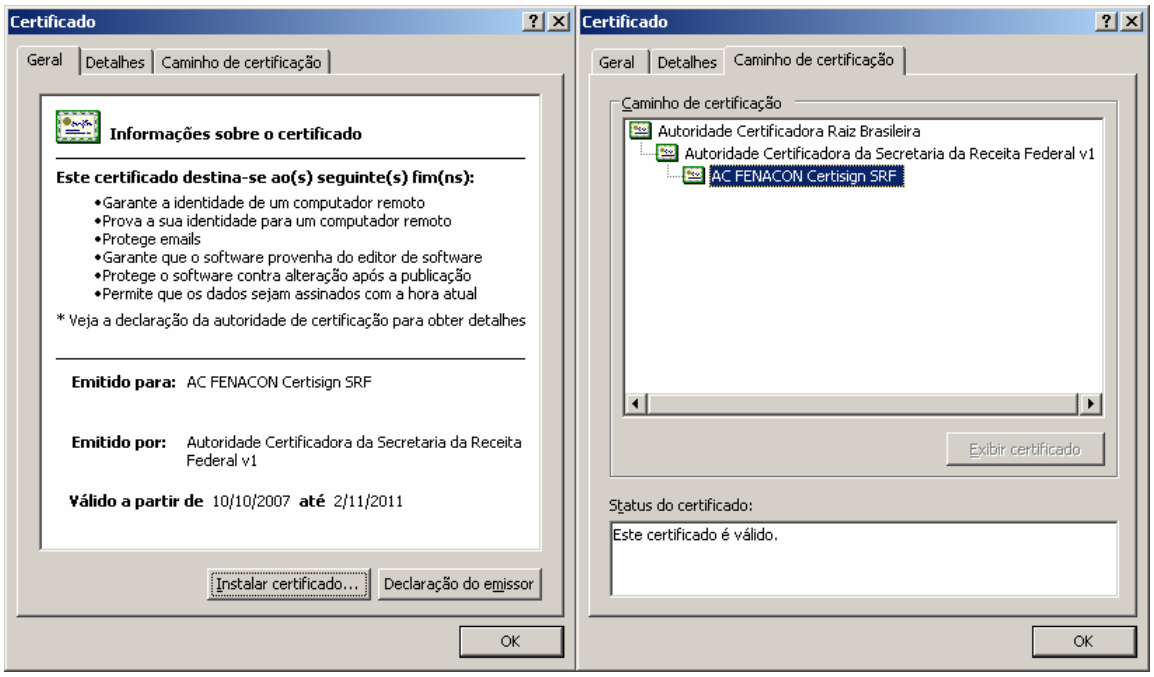

Figura 2 – Certificado da AC-FENACON Certisign e o respectivo caminho de certificação

Fonte: elaborado pelo autor e obtido por meio do próprio certificado digital da AC FENACON Certisign SRF (2009)

Nos dois exemplos citados, observa-se que as entidades que desejam prover serviços eletrônicos de forma segura, têm optado por adotar os CIs para identificar e qualificar os seus usuários.

A crítica existente na centralização das funções de identificação e qualificação em um único certificado é que geralmente a validade de um atributo é diferente da validade de um CI. Além disso, a autoridade que concede um atributo, geralmente não é a mesma que concede o CI (FARRELL et al, 2010, p.2). Por exemplo: uma Autoridade Certificadora (AC) tem a prerrogativa legal de emitir o CI, mas não pode designar o atributo “médico” ao portador, uma vez que esta prerrogativa é do Conselho Federal de Medicina (CFM). Isso resulta em medidas adicionais para que o emissor do CI obtenha as informações de atributos provenientes da fonte de autorização para que possam ser inseridas no CI.

Um dos problemas deste tipo de configuração aparece quando algum campo do certificado é alterado. Nestas situações, existe a necessidade de revogar o

certificado inteiro, o que gera aumento do registro da Lista de Certificados Revogados (LCR) e a necessidade de emissão de um novo CI.

A adoção de um perfil de certificado no qual existe a separação das funções de identificação e de qualificação é chamado de descentralizado (PERMIS, 2007). Neste formato, a identificação fica a cargo de um CI de uma ICP e todos os atributos (qualificadores do usuário) apresentam-se no formato de CA. Esses qualificadores definem os privilégios de acesso dos usuários concedendo-lhes permissões. Esse perfil apresenta vantagens em relação ao centralizado, pois a revogação do CA ocorre independentemente da revogação do CI. Além disso, existem atributos que, dependendo dos requisitos de segurança da aplicação e dos prazos de vigência, dispensam o uso de mecanismos de revogação. Exemplo: um CA de estado civil emitido por um cartório não necessita de controle de revogação, basta que a validade seja pequena (algumas horas segundo, FARRELL et al (2010)) e que o sistema usuário não considere a revogação como algo relevante. Nesta situação, apenas a validade do CA é relevante.

Outra vantagem do CA é a simplicidade da infraestrutura. Serve para qualificar usuários e, assim, não necessita de validação do usuário para sua emissão ou mesmo da sua autorização.

Os serviços eletrônicos que necessitam altos níveis de segurança precisam basicamente de duas verificações: identificação correta do usuário (autenticação) e a concessão dos privilégios aos quais o usuário têm direito de acesso. Uma vez que o processo de identificação ocorra usando um CI, de uso geral e comum para todos os sistemas, os privilégios poderiam ser efetuados pelos mais variados CAs.

A falta de conhecimento do mercado sobre a tecnologia dos CAs está levando as entidades a adotarem este perfil centralizado de certificação digital, com a adoção de CI para efetuar a identificação e qualificação dos usuários.

Uma das motivações da elaboração desta dissertação é evitar que as entidades adotem este caminho complexo e passem a utilizar o CA nos seus mecanismos de qualificação dos usuários.

1.2 Objetivo do trabalho

O objetivo desse trabalho é analisar a aplicabilidade da tecnologia de certificados de atributo, em operação conjunta com os certificados digitais de identidade emitidos no âmbito da ICP-Brasil, apresentando os principais desafios na implementação desta tecnologia, assim como o perfil de uso do certificado de atributo (CA) mais adequado às necessidades das aplicações relacionadas ao processo de autenticação e atribuição de privilégios.

A aplicabilidade pretendida pelo trabalho para o uso do CA baseia-se na análise teórica comparativa entre cenários reais atuais (sem os CAs) e hipotéticos com CAs, relativamente aos itens: segurança, gestão dos certificados e atributos, legalidade e interoperabilidade.

O trabalho analisa também os impedimentos e a dificuldade de implementação dos CAs, que afetariam diretamente na aplicabilidade da tecnologia.

Para uma análise teórica mais realista, foram apresentados e discutidos alguns cenários representativos baseados em quatro estudos de caso.

Os estudos de casos foram escolhidos por apresentarem cenários específicos para cada situação de uso, além de ilustrar as diferentes formas de configuração e uso dos CAs. Alguns dos cenários propõem também a transformação de processos tradicionais em processos eletrônicos.

1.3 Método de trabalho

Inicialmente foram estudados os conceitos relevantes do trabalho. Em seguida foi realizado o levantamento de referências a respeito do estado da arte na área e os atuais sistemas que utilizam os CAs.

O método utilizado pelo trabalho baseia-se em análise teórica de estudos de casos, com comparações entre aplicações reais atualmente em funcionamento, com as mesmas aplicações em um cenário hipotético com o uso dos CAs.

Em cada estudo de caso, a comparação procurou efetuar a análise crítica abordando os seguintes itens:

a) Segurança;

b) Gestão dos atributos e certificados;

c) Legalidade;

d) Interoperabilidade;

Um dos itens que embora seja significativo, mas que não foi possível analisar é a viabilidade econômica de cada modelo proposto. A dificuldade de mensurar os custos envolvidos em uma ICP e uma IGP impediu esta análise.

Pode-se afirmar que construir e manter uma ICP não são triviais. Para exemplificar, para uma entidade se transformar em uma AC da ICP-Brasil, ela deve efetuar o recolhimento de uma taxa de R$ 500.000,00 (ICP-BRASIL, 2006). Além disso, existem outros custos envolvidos na construção da infraestrutura para atender aos requisitos da ICP-Brasil (por exemplo: salas cofres, site de contingência, sistemas de energia elétrica, sistemas de controle de acesso e outros).

Construir e manter uma IGP devem ser menos custosa do que uma ICP, uma vez que os requisitos de segurança são bem menores. Entretanto, neste trabalho, esta é apenas uma constatação empírica sem o levantamento efetivo de todos os custos envolvidos. Partindo-se desta premissa, num cenário ideal, haveria poucas ACs emitindo CIs e várias AAs emitindo CAs, com aplicações vinculadas ou não a mecanismos de identificação baseados em CI. Neste cenário, o custo total seria menor se comparado com o cenário em que toda AA fosse também uma AC, emitindo CI com atributos.

Ao longo da apresentação deste trabalho, observa-se que já existem muitas entidades fazendo exatamente isto, emitindo CIs com atributos quando poderiam estar emitindo apenas CAs.

1.4 Escopo do trabalho

O trabalho irá apresentar a descrição técnica dos certificados de atributos e suas formas de vínculos com os certificados de identidade, além de uma análise dos mecanismos de revogação.

Com a identificação e entendimento de alguns processos não eletrônicos existentes no mundo real, que usam os atributos de uma entidade na concessão de privilégios e também dos processos eletrônicos que utilizam os certificados digitais da ICP-Brasil e os atributos nele contidos, foi possível determinar a escolha dos estudos de casos.

Mais especificamente, serão analisados os estudos de casos nos quais serão apresentadas propostas para o uso da tecnologia de certificados de atributos com as respectivas análises comparativas entre o sistema atual e o proposto.

Esta dissertação sugere alterações nos certificados e-CPF e e-CNPJ com o objetivo de adaptar o seu uso aos CAs, além de sugerir adequações à infraestrutura de gerenciamento de privilégio e ao próprio certificado de atributo para que possa ser usado em conjunto com os certificados de identidade da ICP-Brasil

Esta dissertação não propõe uma nova técnica de uso dos CAs. Os certificados digitais já são padronizados por normas e não é objetivo dessa dissertação propor uma nova ou melhorar o desempenho de alguma técnica já conhecida e nem sugerir alterações nas padronizações.

Também, estão fora do escopo, a criação de protótipos de testes, programas de simulação, análise da criptografia, segurança da criptografia de chaves públicas, análise de vulnerabilidades de uma ICP, análise da vulnerabilidade dos mecanismos de revogação de certificados e questões de ordem jurídica sobre a validade das assinaturas digitais.

No estudo de caso relacionado ao e-CNPJ, as possíveis aplicações apresentadas foram escolhidas para atender às necessidades de funcionamento de uma pequena empresa, uma vez que o objetivo não é cobrir todas as aplicações possíveis, mas de apresentar as possibilidades de uso dos CAs.

1.5 Organização do trabalho

O primeiro capítulo, Introdução, contém a introdução ao assunto a ser tratado com o objetivo e a metodologia adotada na elaboração da dissertação, além da motivação para a sua elaboração.

No segundo capítulo, Revisão Bibliográfica, são apresentadas algumas iniciativas internacionais de uso do CA no processo de definição de permissões de acesso.

No terceiro capítulo, Os Certificados Digitais, são descritos os componentes de uma IGP, de uma ICP e da forma de interação que pode ocorrer entre estes dois tipos de certificados.

O quarto capítulo, Os Certificados de atributo e o certificado de identidade na ICP-Brasil, proporciona uma análise geral de como um CA poderia interagir com o certificado da ICP-Brasil.

O quinto capítulo, Os Certificados de atributo e o certificado de identidade na ICP-Brasil, apresenta os motivos que levaram a escolha de cada um dos casos para serem objetos de estudos.

O sexto capítulo Estudo de Caso: Certificação digital da OAB, trata de um estudo para que entidades de classe como a OAB, possam oferecer certificados de atributos aos seus advogados associados e quais os benefícios e desafios desta implementação em relação ao sistema atual em curso.

O sétimo capítulo Estudo de Caso: Cadastro de Pessoa Física (CPF), discute sobre o atual perfil do atributo CPF, tanto em formato convencional quanto em formato eletrônico (e-CPF) e propõe alterações neste perfil para o uso dos CAs para este atributo.

O oitavo capítulo, Estudo de Caso: e-CNPJ, trata sobre algumas aplicações relacionadas a pessoas jurídicas, nas quais é possível adotar os CAs.

O nono capítulo, Estudo de Caso: Prontuário Eletrônico de Paciente (PEP), avalia o uso dos CAs no atual sistema de certificação dos Sistemas de Registro Eletrônico de

Saúde (S-RES) realizado pela Sociedade Brasileira de Informática em Saúde (SBIS) em conjunto com o Conselho Federal de Medicina (CFM).

O décimo capítulo, Conclusão, traz o resultado do trabalho realizado contendo um resumo geral dos objetivos do trabalho, as conclusões, as contribuições e os trabalhos futuros que podem ser abordados sobre o assunto tratado.

2 REVISÃO BIBLIOGRÁFICA

2.1 Introdução

Um certificado digital de identidade (CI) são estruturas de dados que associam uma chave pública a uma entidade. Esta associação é assegurada por meio de uma assinatura digital presente no certificado, realizada por uma autoridade certificadora confiável. A autoridade certificadora pode fundamentar esta associação por meios técnicos (conhecido como método para comprovar a posse de chave privada), por meio da apresentação da chave privada ou por uma declaração da entidade (HOUSLEY, 2002). Um CI contém os dados de seu titular, tais como: nome e e-mail do titular e nome e assinatura da AC que o emitiu.

Diversas organizações e entidades têm a necessidade de disponibilizar serviços eletrônicos que requeiram um alto nível de segurança. Com os certificados digitais de identidade, isto se torna possível. Porém, para estes serviços serem seguros eles devem, além de identificar corretamente o usuário, liberar apenas o acesso aos recursos que o usuário tem autorização. Em um exemplo hipotético de uma aplicação médica, o sistema somente liberaria a tela para a assinatura de um laudo após a identificação e qualificação do médico.

Em outro exemplo hipotético, uma transação de um sistema de petição eletrônica de um tribunal poderia ser realizada de forma segura por meio de um certificado de identidade (CI) e só deveria permitir o acesso nas situações em que o usuário fosse um advogado qualificado (inscrito na OAB, ter a procuração, etc.).

Estes exemplos ilustram situações em que os serviços de autenticação e de autorização são necessários podendo ser realizados por meio de dois formatos de certificados:

a) usando apenas o CI: a autenticação do usuário é realizada pelo CI e a autorização é dada por meio da verificação de campos que compõem o certificado (ser médico ou ser advogado);

b) usando um CI e um CA: a autenticação do usuário é realizada pelo CI e a autorização por meio da verificação dos campos do CA.

Os certificados digitais de identidade foram definidos na terceira versão do padrão X.509 publicado pela *International Telecommunication Union Telecommunication Standardization Sector* (ITU-T, 1997). Ele é um tipo de certificado de Infraestrutura de Chave Pública (ICP), sendo o mais usual o formato definido pela RFC 5280 (COOPER et al, 2008).

Os CAs foram definidos na quarta versão do padrão X.509 publicado pela *International Telecommunication Union Telecommunication Standardization Sector* (ITU-T, 2000). Ele é um tipo de certificado digital usado em Infraestrutura de Gerenciamento de Privilégios (IGP). A IGP é para a autorização o que a ICP é para a autenticação, conseqüentemente, existem vários conceitos similares entre as ICPs e as IGPs (Tabela 1).

A entidade que assina um CI é chamada de Autoridade Certificadora (AC) e a entidade que assina um CA é chamada de Autoridade de Atributo (AA). A raiz de confiança de um ICP é chamada de AC Raiz e a raiz de confiança de uma IGP é chamada de Fonte de Autoridade de Atributo (FAA). As ACs podem confiar e delegar poderes de autenticação e certificação para ACs subordinadas. Do mesmo modo, as FAA podem delegar os seus poderes de autorização para AAs subordinadas. Se um usuário precisar revogar o seu CI, a AC publicará esta informação na sua Lista de Certificados Revogados (LCR), e se um usuário precisa ter um atributo revogado, a AA o fará por meio de uma Lista de Certificados de Atributos Revogados (LCAR).

Tabela 1 - Comparação entre ICP e IGP

Conceito	Entidade da ICP	Entidade da IGP
Tipo de Certificado	Certificado de Identidade (CI)	Certificado de Atributo (CA)
Emissor do Certificado	Autoridade Certificadora (AC)	Autoridade de Atributo (AA)
Usuário do Certificado	Titular do CI	Titular do CA
Relação definida no Certificado	Titular ⇔ chave pública	Titular ⇔ atributo
Revogação	Lista de Certificados Revogados (LCR)	Lista de Certificados de Atributos Revogados (LCAR)
Raiz de confiança	AC Raiz	Fonte de Autoridade de Atributo
Autoridade subordinada	AC subordinadas	Autoridade de Atributo

Fonte: CHADWICK (2002)

Os CAs com perfil de uso na Internet foram definidos pela RFC 5755 (FARRELL et al, 2010). Ele é um certificado que contém algum tipo de relação (ou vínculo) de um atributo a um usuário. Este vínculo geralmente é realizado por meio de um identificador único do usuário ou por meio de uma referência explícita ao certificado de identidade do usuário. Além disso, o CA deve conter um ou mais atributos que se queira designar ao portador. Esse certificado deve ser assinado digitalmente por meio do CI da AA, entidade que detém a prerrogativa de designar o atributo ao usuário.

Diferentemente dos CIs, os CAs não têm um par de chaves e, portanto não são usados para a autenticação de um usuário. Os CAs apenas indicam os atributos de um determinado indivíduo – por exemplo, se ele é um advogado, se é um motorista, se é eleitor, se tem plano de saúde, etc. Este tipo de certificado se usado em

conjunto com um CI, pode ser usado para uma identificação e qualificação segura de uma entidade.

O CA tem a sua própria validade e, assim como o CI, pode também ser revogado. Para revogação, a AA pode optar por manter, ou não, uma Lista de Certificados de Atributos Revogados, dependendo do tipo de aplicação e do prazo de validade dos certificados.

Uma das características do CA é que ele pode ser emitido sem a presença do usuário, pois como não existe a chave privada, não há a necessidade de autenticação. Uma entidade como o Departamento de Trânsito (DETRAN) poderia emitir uma carteira de habilitação em formato de CA, apenas constando no certificado, que a pessoa (identificado, por exemplo, pelo seu emissor + RG) é um motorista habilitado.

Estas características fazem com que uma IGP seja uma estrutura bem mais simples do que uma ICP. Isto significa que quanto mais entidades optem pelo uso dos CAs ao invés dos CIs, mais simples será a estrutura total que compõe a certificação digital do país.

O CA tem sido usado com sucesso há alguns anos na Espanha (ICAM, 2007). As possibilidades de aplicação do CA são bastante extensas, embora ainda pouco exploradas. A outra vantagem importante do CA é a completa preservação do CI nos casos de revogação do atributo. A pessoa pode ter um atributo revogado (deixar de ser funcionário, motorista, eleitor, advogado, etc.) e mesmo assim o seu CI manter-se válido.

O Instituto Nacional de Tecnologia da Informação – ITI ainda está estudando a adoção dos CAs (ITI, 2008) dentro do âmbito da ICP-Brasil.

2.2 Trabalhos relacionados

Nesta seção são apresentados alguns trabalhos relevantes relacionados ao tema.

2.2.1 PERMIS

O projeto PERMIS (*PrivilEge and Role Management Infrastructure Standards validation*) foi financiado pela Comissão Européia e teve como objetivo construir uma IGP baseada em certificados X.509 para que pudesse ser utilizada por três cidades euroéias. As cidades escolhidas para participarem deste projeto foram Barcelona (Espanha), Bologna (Itália) e Salford (Reino Unido).

Todas as três cidades já possuíam experiências de uso com CI e por este motivo era natural que elas desejassem adicionar a capacidade de gerenciamento de privilégios a fim de completar os mecanismos fortes de autenticação e de autorização.

As aplicações selecionadas eram bastante diferentes e por este motivo ilustravam a generalidade que uma IGP podia alcançar.

No caso de Bolonha, a cidade desejava liberar o acesso aos arquitetos para eles pudessem atualizar os mapas da cidade com o objetivo de planejar a construção de novas edificações e assim melhorar o planejamento do crescimento da cidade. A automatização deste processo melhorou significativamente a eficiência, pois até então este processo era realizado por meio de remessas para a prefeitura da documentação impressa executada pelos correios.

Barcelona é uma cidade turística e como tal possui muitas empresas locadoras de veículos. Entretanto, estacionamento é um item bastante escasso e freqüentemente são emitidas multas para veículos alugados. Desta forma era bastante comum que quando a multa chegava à locadora de veículos, o locatário já havia deixado o país. O projeto pretendeu fornecer às locadoras de veículos acesso on-line ao banco de dados de multas para que a empresa pudesse verificar rapidamente a situação do veículo no momento em que fosse realizada a sua devolução. A necessidade de segurança no acesso era devida porque as locadoras somente podiam ter acesso às multas dos veículos da sua frota.

Em Salford pretendeu-se implementar um sistema eletrônico para licitação pública (SALFORD, 2007). O processo era iniciado quando a cidade publicava uma nova licitação pública, solicitando propostas aos fornecedores, permitindo que qualquer fornecedor pudesse ter acesso a ela por meio da internet. Porém, em alguns casos

apenas fornecedores autorizados podiam enviar propostas, ou em outros casos, a exigência poderia ser que a empresa possuísse certificações de qualidade.

O desafio do Projeto PERMIS era construir uma IGP baseada em certificados X.509, que pudessem servir para uma ampla variedade de aplicações. No PERMIS existiam três componentes principais para a montagem da IGP: a política de autorização, o alocador de privilégios (PA) e a interface de programação da IGP (API).

A política de autorização especificava quem acessava, qual o tipo de acesso, quais objetos eram acessados e sob quais condições.

O sistema de autorização baseada em políticas por domínio é preferível a ter ACL (*Access Control List*) configuradas separadamente para cada objeto. As ACLs são mais difíceis de serem administradas, pois duplica o esforço dos administradores (uma vez que deve ser repetido em cada objeto) e é menos seguro pela dificuldade de manter um registro de quais direitos de acesso o usuário tem em todo o domínio.

Por outro lado, a autorização baseada em política permite que o administrador do domínio (a fonte de autoridade) especifique a diretiva de autorização para um conjunto de domínios e todos os objetos que podem ser protegidos por um mesmo conjunto de regras.

O Projeto PERMIS adotou o modelo RBAC (*Role-Based Acces Control*) hierárquico para especificar autorizações. O RBAC tem a vantagem de possuir escalabilidade em relação ao modelo de controle de acesso discricionário (*discretionary access control* – DAC) e pode lidar com grandes números de usuários uma vez que, normalmente, existem muito menos papéis do que usuários (CHADWICK, 2002).

O Projeto PERMIS quis especificar o política de autorização em uma linguagem que pudesse ser facilmente analisada por computadores e lido pelas SOAs (*Source Of Authority*) com ou sem ferramentas de software. O XML (*eXtensible Markup Language*) foi a linguagem escolhida para esta especificação por existirem muitas ferramentas disponíveis, além do que a linguagem estava se tornando rapidamente um padrão de mercado, sendo possível de ser lido e entendido pela maioria dos técnicos, diferentemente do ASN1 (*Abstract Syntax Notation One*) que usa codificação binária.

Inicialmente foi criada uma DTD (*Document Type Definition*) para a política X.500 de IGP-RBAC. O DTD era uma metalinguagem em XML que continha as regras para a criação de políticas de autorização. O DTD compreendia a seguintes componentes:

a) *SubjectPolicy* - especifica os domínios, ou seja, quais os domínio cobertos pela política;

b) *RoleHierarchyPolicy* - especifica os diferentes papéis e os seus relacionamentos hierárquicos;

c) *SOAPolicy* - especifica quais SOAs são confiáveis para atribuir papéis;

d) *RoleAssignmentPolicy* - especifica quais papéis podem ser atribuídos ao titular e por quais SOAs, se a delegação de funções pode ocorrer ou não, e por quanto tempo os papéis podem ser atribuídos;

e) *TargetPolicy* - especifica os domínios de destino que são cobertos pela política.

f) *ActionPolicy* - especifica as ações ou métodos que são suportadas pelos objetos de destino, além dos parâmetros que devem ser passados com cada ação;

g) *TargetAccessPolicy* - especifica quais papéis têm permissão de executar determinadas ações, em certos objetos e sob quais condições. As condições são especificadas usando lógica booleana e pode conter restrições. Todas as ações que não especificadas na política de acesso alvo são negadas.

O SOA criava uma política de autorização para o domínio usando sua ferramenta de edição preferida em XML e armazenava em um arquivo local para ser acessado posteriormente pelo *Privilege Allocator* (PA).

O PA era uma ferramenta utilizada pelo SOA ou AA para atribuir privilégios aos usuários. Uma vez que o PERMIS usava o RBAC, o SOA utilizava a PA para atribuir papéis aos usuários na forma de CA para a definição de papéis. Os CAs eram emitidos a todos os usuários das aplicações das cidades escolhidas.

No caso de Bolonha, havia dois papéis: “leitor de mapa” e “arquitetos”. Leitores de mapas podiam fazer *download* de quaisquer mapas produzidos pelo município, enquanto que os arquitetos estavam autorizados a fazer *download* e *upload* de mapas modificados digitalmente.

No caso de Barcelona, havia também dois papéis: “generalizado” e “autorizado”. Qualquer cidadão ou empresa podia ter o papel “generalizado”. Qualquer pessoa com o papel “generalizado” tinha a permissão de ver as suas próprias multas. As empresas com contrato com o município tinham o papel “autorizado”. As empresas com o papel “autorizado” podiam ler as suas próprias multas e também modificar os detalhes das mesmas, por exemplo, atualizar o nome do condutor e o endereço.

Em Salford era diferente dos outros sites, embora atribuísse dois papéis - a de “candidato” e apresentação de propostas “oficial” - que também contava com uma SOA externa. Neste caso a *British Standards Institution* (BSI) - para atribuir o papel da certificação ISO 9000 (*International Organization for Standardization)* para os usuários. No projeto, o plano era criar uma procuração do BSI para que a prefeitura pudesse agir em nome da BSI, uma vez que BSI não participava do projeto.

Uma vez que a atribuição de papéis havia sido realizada por meio de CA emitido pelo PA, estes certificados eram armazenados em um diretório *Lightweight Directory Access Protocol* (LDAP). Visto que os ACs são assinados digitalmente pela AA emissora, eles são invioláveis e, portanto, não havia risco em permitir que eles fossem armazenados em um diretório LDAP acessível ao público.

Isto significava também que as AAs que emitiam CAs podiam armazená-los localmente e dar acesso global para eles. Isto poderia ser particularmente útil no caso dos certificados de ISO 9000, por exemplo. Qualquer pessoa que quisesse saber se uma entidade possuía o ISO 9000 poderia consultar o diretório LDAP da BSI e recuperar o CA. A LCAR se houvesse, também seria armazenada aqui. Assim, em geral, era pequena a vantagem de distribuir os CAs aos seus titulares, uma vez que uma terceira parte confiável ainda precisaria de acesso ao diretório LDAP da entidade emissora para recuperar a última LCAR.

Outra função do PA era criar uma política de autorização que fosse assinada digitalmente como um Certificado de Atributo de Política (CAP). O CAP era um CA

no padrão X.509 com a seguinte característica especial – o titular e o emissão eram os mesmos, ou seja, a própria AA. Neste tipo de CA o tipo de atributo é o pmiXMLPolicy e o valor do atributo é a política XML criada anteriormente. O PA solicitava à AA o nome de arquivo da política e, em seguida, copiava o conteúdo para o valor do atributo. Depois que a AA assinasse o CAP, o PA o armazenava no seu diretório LDAP.

A generalidade do projeto PERMIS mostrou o seu valor na medida em provou ser adaptável em diversos cenários. Com a definição adequada das políticas de autorização o ADF era capaz de decidir com segurança se um determinado usuário detentor de um papel podia executar uma ação sobre um objeto.

A análise do PERMIS demonstra a viabilidade do modelo de autorização baseado em papéis (RBAC) em uma IGP. Além de mostrar também que é possível usar CAs em processos seguros de atribuição de privilégios.

2.2.2 ICAM – Ilustre Colegio de Abogados de Madri

Na Espanha a Infraestrutura de Chaves Públicas é controlada pela CERES (*Autoridad Pública de CERtificación ESpañola*) que é uma entidade ligada à *Fábrica Nacional de Moneda y Timbre (FNMT)* subordinada ao *Ministerio de Economia y Hacienda*. A CERES é a autoridade raiz e existem outras quinze autoridades certificadoras. Abaixo delas estão mais de 3500 autoridades de registro fazendo a verificação de identidade dos cidadãos. As informações ilustram a evolução da ICP no país (GALLARDO, 2006):

- Agosto de 2004 – 580.000 certificados ativos;
- Agosto de 2005 – 750.000 certificados ativos;
- Agosto de 2006 - 1 milhão de certificados ativos;
    - Mais de 3.500 escritórios de registro para verificação de identidade;
    - 15 Autoridades Certificadoras;
    - 16 Ministérios, dos quais 14 utilizam o certificado;
    - 8108 Prefeituras, das quais 6068 utilizam o certificado.

Os CAs têm sido utilizados com sucesso na Espanha desde 2004 pela *ICAM – Ilustre Colegio de Abogados de Madrid* (a equivalente espanhola da OAB). O "*Certificado de Abogado Ejerciente*" expedido pela ICAM é um CA que permite aos advogados inscritos confirmar a sua condição de advogado em atividade nas transações eletrônicas efetuadas à distância.

O "*Certificado de Abogado Ejerciente*" é um certificado independente que está vinculado ao CI de pessoa física da FNMT (ICP-Espanha). Desta forma a revogação do CA, não afeta a validade do CI que pode continuar a ser utilizado nas aplicações de um cidadão comum.

Em fevereiro de 2006, a Comunidade de Madri (*La Comunidad de Madrid*) e a ICAM, firmaram um convênio para estabelecer a relação de confiança dos CAs emitidos pela ICAM. A Comunidade de Madri é uma comunidade autônoma da Espanha composta pelas províncias de Guadalajara, Cuenca, Toledo, Ávila e Segovia. Com este convênio, a Comunidade de Madri proporcionará aos advogados da ICAM a capacidade de atuar como tal nos serviços que exijam a condição de advogado ativo. Isto envolverá um conjunto de serviços eletrônicos em que seja necessária a identificação da pessoa e do advogado.

Atualmente, já é possível assinar digitalmente qualquer documento eletrônico que necessite da identificação explícita como advogado membro da ICAM. Estes documentos eletrônicos assinados digitalmente podem ser transmitidos por meios eletrônicos com a mesma validade de um documento no papel, com a garantia de ter sido elaborado por um advogado ativo e de modo seguro

A experiência do ICAM mostra a possibilidade de uso dos CAs em um ambiente real. O mecanismo de autorização dos sistemas usa o CA de advogado para a liberação de recursos e o mecanismo de autenticação utiliza o CI emitido pela FNMT. Desta forma, os sistemas que necessitam realizar transações seguras (principalmente o judiciário) conseguem se beneficiar com o uso dos dois certificados.

2.2.3 Um modelo de controle de acesso a recursos de rede baseado em ICP e IGP

ARREBOLA (2006) mostrou as vantagens da separação dos serviços de autenticação e autorização em duas infraestruturas separadas, a ICP e IGP. Estas vantagens são obtidas com relação à facilidade de administração, além da possibilitar uma maior granularidade do sistema de autorização.

Neste trabalho foi apresentado um protótipo de uma aplicação com a integração das duas infraestruturas. Desta forma, aumentou-se o nível de segurança às aplicações, nos quesitos autenticação e autorização.

O uso de certificados padronizados (X.509) fizeram com que o modelo fosse extensível às outras aplicações que porventura venham a utilizar os mesmos certificados.

A principal diferença observada entre o modelo proposto por ARREBOLA (2006) e o projeto PERMIS é que neste último não existe a necessidade de uso do CI (ICP) para o mecanismo de autenticação.

Outro ponto observado por ARREBOLA (2006) foi a dificuldade da implementação prática dos mecanismos de delegação previstos no formato do CA (FARRELL et al, 2010), uma vez que esta tarefa é bastante dispendiosa e complexa, sobretudo para a validação dos caminhos de certificação envolvidos no processo.

3 OS CERTIFICADOS DIGITAIS

3.1 Infraestrutura de Chaves Públicas

Uma Infraestrutura de Chaves Públicas (ICP) ou *Public Key Infrastructure (PKI)* é um conjunto de técnicas, práticas e procedimentos para a implementação e operação de um sistema de emissão de certificados digitais baseado na criptografia assimétricas de chaves (ROLT et al, 2006). A ICP baseia-se no princípio da terceira parte confiável, o qual oferece a mediação de acreditação e confiança entre as partes que usam o sistema de certificados digitais.

Esse sistema é a técnica mais recomendável para garantir a autenticidade confiável de uma entidade (VILLAR et al, 2004).

3.1.1 Os serviços envolvidos em uma ICP

Os serviços envolvidos em uma ICP são:

a) emissão dos certificados;

b) gerenciamento e armazenamento dos certificados;

c) distribuição de certificados;

d) renovação de certificados;

e) suspensão e revogação de certificados.

3.1.2 Componentes básicos de uma ICP

Os componentes básicos de uma ICP são:

a) Autoridade Certificadora (AC) – entidade confiável que emite os certificados digitais de identidade e fazem a guarda em repositório;

b) Autoridade de Registro (AR) – verifica a autenticidade da pessoa e autoriza a emissão do certificado digital de identidade;

c) LCR – lista de certificados revogados, mantida pela AC;

d) Certificado Digital de Identidade – chave pública do titular, emitido pela AC e assinado digitalmente por ela usando sua chave privada.

3.1.3 Certificado Digital de Identidade

Um certificado digital de identidade é um documento eletrônico que contém um conjunto de informações referentes à entidade para o qual o certificado foi emitido (seja uma empresa, pessoa física ou computador) mais a chave pública referente à chave privada de posse unicamente da entidade especificada no certificado (ITI, 2005). Esse documento é assinado digitalmente por uma terceira parte confiável, a autoridade certificadora que faz a ponte de confiança do vínculo da chave pública à identidade da entidade que detém a chave privada correspondente. A assinatura digital do emissor certifica a validade da ligação entre a chave pública e as informações de identificação do requerente.

Existem diversos usos para os certificados digitais de identidade e os seguintes exemplos descrevem algumas situações de uso:

a) um usuário deseja acessar um *site* de Internet com conexão segura como, por exemplo, acessar a sua conta bancária. É possível verificar se o site acessado é realmente da instituição que se diz ser, por meio da checagem do certificado digital e da obtenção segura da chave pública;

b) de forma oposta à anterior, o servidor acessado necessita uma identificação segura do usuário, como por exemplo, o site da Receita Federal na entrega de imposto de renda. Nessa situação, o certificado digital do usuário é apresentado na autenticação do usuário e o servidor obtém a chave pública do usuário;

c) o envio de uma mensagem de correio eletrônico com autoria comprovada. O remetente assina digitalmente a mensagem, assegurando que o conteúdo não seja alterado durante o transporte, ou se o for, seja facilmente identificável. O destinatário valida o certificado de identidade do remetente e obtém a chave pública para realizar a validação do conteúdo;

d) o envio de uma mensagem confidencial de correio eletrônico, no qual apenas o destinatário pode ter acesso. O remetente cifra a mensagem usando a chave pública do destinatário obtida após a validação do certificado digital do usuário. Desta forma apenas o destinatário, portador da chave privada pode decifrar a mensagem, assegurando que o conteúdo não foi lido por terceiros durante o transporte.

e) a instalação de um aplicativo no computador e a verificação da autenticidade da autoria do programa. Usa-se o certificado de identidade do fabricante para assinar digitalmente o programa.

Um certificado só é válido pelo período de tempo nele especificado. Após o período de validade, o usuário deve solicitar um novo certificado. Nos casos em que seja necessário revogar o certificado, o usuário deve solicitar à AC a revogação do certificado. Todos os certificados revogados são publicados na Lista de Certificados Revogados (LCR) que é mantida por cada AC.

3.1.4 Domínio de Confiança

O “Domínio de Confiança” é a área lógica da abrangência, sob o ponto de vista do usuário, no qual existe a relação de confiança entre o usuário e as autoridades certificadoras raízes.

Por exemplo: um certificado emitido sob a ICP-Brasil está no “Domínio de Confiança” de um usuário, desde que o mesmo considere a AC raiz da ICP-Brasil como uma AC confiável.

3.1.5 Cadeia de Certificação

“Cadeia de Certificação” é uma série hierárquica de certificados assinados por sucessivas ACs. Essas interligações existentes entre as diversas ACs são chamadas de Cadeia de AC.

3.1.6 Validade do Certificado

Um certificado é considerado válido quando passa pela validação criptográfica, está dentro do prazo de validade, não foi revogado e, sendo possível validar todos os certificados da cadeia de certificação até atingir uma AC raiz, no qual o usuário confia, ou seja, que pertence ao seu domínio de confiança.

3.1.7 Revogação

Toda a segurança do processo de assinatura digital parte do pressuposto de que a chave privada está em poder exclusivo do seu titular. No caso da chave privada estar em mãos alheias, este terceiro poderá produzir assinaturas digitais como se fosse o verdadeiro titular das chaves, não havendo meios técnicos de se demonstrar a falsidade.

Por isso, quando houver suspeita de que a chave privada foi comprometida, deve-se pedir a revogação do certificado à AC emitente (COOPER et al, 2008, p.100).

Outra situação que exige a revogação do certificado é a perda da chave privada. Se, por qualquer motivo, o titular perder o acesso à sua própria chave privada, não há meios de recuperá-la. Neste caso, o certificado deve ser revogado para que outro possa ser solicitado. Para esta situação, existe também um estado intermediário de revogação chamado “hold”, o qual permite a suspensão temporária do certificado, pois não se tem a confirmação de perda da chave de privada. Nesta situação, quando o usuário retoma acesso à chave privada, o certificado pode voltar a ficar ativo (COOPER et al, 2008, p.63).

Existem outras duas situações que produzem a revogação de um certificado: a retirada do titular do domínio de confiança ou na situação em que alguma informação no certificado esteja incorreta.

Todo mecanismo de autenticação que usa certificados digitais de identidade deve verificar a revogação, sob risco de aceitar um certificado inválido. Existem atualmente dois meios de se identificar um certificado revogado: por meio da Lista de Certificados Revogados (LCR) (COOPER et al, 2008) ou por meio do protocolo Online *Certificate Status Protocol* (OCSP) (MYERS et al, 1999).

3.1.8 Lista de Certificados Revogados

Nas operações dos sistemas criptográficos que usam a infraestrutura de chaves públicas existe um componente denominado Lista de Certificados Revogados (LCR). A LCR contém a relação dos números de série dos certificados que foram revogados, os quais não são mais válidos e não devem ser aceitos pelos sistemas.

A LCR é mantida e publicada pela AC. Ela é assinada digitalmente pela emitente de forma a possibilitar a verificação da sua integridade e origem. A lista, geralmente, contém o nome de quem a emite, a data de emissão e a data da próxima emissão programada, além dos números de série dos certificados revogados e a data da revogação.

A LCR deve ser atualizada com uma freqüência pré-definida e bem determinada. A freqüência de atualização de uma LCR depende do que foi definido nas políticas de segurança da AC. Opcionalmente, uma LCR pode ser publicada antes do tempo previsto, imediatamente após a revogação de um certificado.

Para poder confiar em um certificado, uma aplicação deve verificar se o seu número de série não consta na LCR publicada pela AC. Para isto, a aplicação deve manter em sua base de dados a LCR mais atual ou baixar a versão mais recente a cada solicitação.

A LCR pode se tornar ponto de vulnerabilidade de uma ICP, pois a incorreta manutenção das informações das LCRs pode incorrer em aceitação de certificados revogados. Isto significa que para a efetiva segurança das transações que usam a ICP, a LCR deve estar sempre acessível. A necessidade de efetuar as consultas on-line às LCRs para a verificação da validade vai contra uma das vantagens iniciais da ICP quando comparadas com os mecanismos de autenticação de chaves simétricas, pois nos dois sistemas existe, a necessidade de um serviço on-line de validação. Esta necessidade de consulta é um alvo em potencial para ataques de negação de serviço, pois se um certificado não puder ser verificado quanto à sua validade, então ele não poderá ser aceito.

Além disso, a existência de uma LCR implica na necessidade do titular seguir as políticas de revogação.

3.1.9 *Online Certificate Status Protocol*

Com um crescente número de usuários e a revogação freqüente de certificados as LCRs podem tornar-se excessivamente grandes causando lentidão da sua obtenção do repositório e causando impacto de tamanho no seu armazenamento. Uma alternativa viável para complementar ou mesmo substituir as listas de certificados revogados é a utilização do protocolo *Online Certificate Status Protocol* (OCSP) (MEYERS et al, 1999).

Por meio do OCSP, qualquer aplicação pode fazer consultas a um serviço que verifica o estado de um determinado certificado, mantido pela AC. As respostas emitidas, específicas para um determinado certificado são assinadas digitalmente pela AC, a fim de garantir sua confiabilidade. A principal vantagem do OCSP apontada por MARTINS (2003) é o tamanho das mensagens.

3.2 Infraestrutura de Gerenciamento de Privilégios

A Infraestrutura de Gerenciamento de Privilégios (IGP) pode ser definida como um conjunto de processos para fornecer o serviço de autorização. Esse serviço atua em conjunto com os certificados de identidade no padrão X.509 definido pela RFC 5280 (COOPER et al, 2008), que define formatos de dados e procedimentos relacionados à distribuição das chaves públicas por meio de certificados assinados digitalmente por uma AC.

Uma IGP é semelhante à infraestrutura de chaves públicas.

3.2.1 Componentes básicos de uma IGP

Os componentes básicos de uma IGP são:

a) Certificado de Atributo;

b) Fonte de Autoridade de Atributo;

c) Autoridade de Atributo;

d) Lista de Certificados de Atributos Revogados.

3.2.2 Certificado de Atributo

Um certificado de atributo (CA) é um documento digital assinado eletronicamente por uma Autoridade de Atributo (AA), que apresenta qualidades associadas ao titular do CA.

O CA é um tipo de certificado usado para designar qualidades a uma entidade. Diferentemente dos certificados digitais de identidade, os CAs não têm um par de chaves e, portanto, não podem ser usados para a autenticação de um usuário. Os CAs apenas indicam os atributos de uma entidade. Por exemplo, se um indivíduo é um advogado, motorista, eleitor qualificado, se tem plano de saúde, etc. Em conjunto com um CI (como o e-CPF), o CA pode ser usado para a correta identificação e qualificação de um indivíduo.

Os CAs foram definidos pela RFC 5755 (FARRELL et al, 2010). Ele é um certificado que contém simplesmente um campo de identificação do titular (campo vinculante) e um conjunto de atributos que se queira designar ao titular. Esse certificado é assinado digitalmente por uma Autoridade Atributos (AA), que seja considerada confiável para designar aquele atributo. Por exemplo, a Ordem dos Advogados do Brasil (OAB) é confiável para designar o atributo de advogado e o Tribunal Regional Eleitoral (TRE), o atributo de eleitor.

O vínculo entre o CI e o CA pode ser realizado pelo número de série e emissor do certificado, ou por qualquer outro campo único de identificação do usuário como, por exemplo, o número do RG associado ao emissor ou o número do Registro Único de Identidade Civil (RIC). Os CAs têm a sua própria validade e, assim como o CI, podem também serem revogados.

Uma das características dos CAs é que eles podem ser emitidos sem a presença do usuário pois, como não existe a chave privada, não há segredo e nem a necessidade de autenticação. Uma entidade como o Departamento de Trânsito

(DETRAN), poderia emitir uma carteira de habilitação em formato de CA, apenas constando no certificado, que um determinado usuário é um motorista habilitado.

3.2.2.1 Estrutura do Certificado de Atributos

1. version	
2. holder	
3. issuer	
4. signature	
5. serialNumber	
6. attrcertValidityPeriod	notBeforeTime
	notAfterTimer
7. attributes	
8. issuesUniqueID	
9. extensions	
10. Attribute Authority signature	

Figura 3 - Estrutura do Certificado de Atributo

Fonte: FARREL et al (2010)

3.2.2.1.1 Version

Este campo deve ter o valor v2, que é a versão da codificação DER.

A versão v2 não é compatível com a versão anterior v1 definida em 1997.

3.2.2.1.2 Holder

O *Holder* representa a entidade titular de um atributo. O titular pode ser representado de três formas: *baseCertificateID, entityName e objectDigestInfo*.

Com a opção *baseCertificateID*, os campos *serialNumber* e o is*suer* devem ser iguais ao campo *Holder* do CA. O *issuer* do CI deve ser preenchido com um único valor de *holder.baseCertificateID.issuer* do campo *directory Name*.

O campo *holder.baseCertificateID.issuerUID* do CA deve ser usado apenas se o campo *holder* do CI contiver o campo *issuerUniqueID*. Se o campo *holder.baseCertificateID.issuerUID* do CA e o campo *issuerUniqueID* do CI estiverem presentes, o mesmo valor deve estar nos dois campos.

Se o campo *holder* usar a opção *entityName* e o autenticação for baseado em um CI, o campo *entityName* deve ser igual ao campo *subject* do CI, ou um dos valores da extensão *subjectAltName*. O uso da extensão *subjectAltName* só é obrigatória quando o campo *subject* estiver vazio. Nesta opção podem ocorrer colisões com o nome das entidades.

Nas situações em que as opções *baseCertificateID* e *entityName* não forem usadas, pode-se usar o campo *objectDigestInfo*. A idéia desta opção é conectar o CA ao *hash* da chave pública ou ao *hash* do CI.

Se for usado o *hash* de chave pública, deve-se usar o campo *SubjectPublicKeyInfo* como base para o cálculo do *hash*.

Se for usado o *hash* do CI, deve-se usar o CI inteiro como entrada para o cálculo do *hash*, incluindo a assinatura.

3.2.2.1.3 Issuer

O campo issuer deve conter um nome único de emissor apenas.

3.2.2.1.4 Signature

Contém o identificador dos algoritmos usado para validar a assinatura do CA. Os algoritmos são definidos pela RFC 3279 (POLK et al, 2002).

3.2.2.1.5 Serial Number

Para qualquer CA, o conjunto *issuer* + *serialNumber* deve ser único, mesmo que o certificado tenha curta validade.

O *serialNumber* deve ser um número inteiro e positivo seqüencial com um limite máximo de até 20 octetos.

3.2.2.1.6 Período de Validade

O campo *attrCertValidityPeriod* define o período de validade do CA.

O formato segue o padrão ASN.1 e devem ser expressas em UTC (Universal Time Coordinated) AAAAMMDDHHMMSSZ.

3.2.2.1.7 Atributos

Os campos atributos fornecem informações sobre o titular do CA. Quando o CA é usado para autorização, freqüentemente os atributos contém um conjunto de privilégios. Um CA deve conter pelo menos um atributo.

3.2.2.1.8 Identificador único do emissor

Este campo não pode ser usado a menos que seja também usado no campo *issuer* do CI. Neste caso ambos devem ser preenchidos.

3.2.2.1.9 Extensões

Os campos de extensões geralmente são usados para fornecer informações sobre um CA. Um CA sem extensões está de acordo com o padrão RFC 5755 (FARRELL et al, 2010), entretanto existem algumas extensões as quais, quando usadas, são consideradas como críticas. Nestas situações, estes campos devem ser preenchidos, pois senão o CA estará fora do padrão definido pela RFC 5755 (FARRELL et al, 2010).

As extensões presentes nos CAs provêm métodos adicionais de associação entre os titulares dos CA e seus atributos.

As extensões são campos que podem ser usadas livremente pelas entidades, podendo carregar qualquer tipo de informação relevante ou não. O cuidado que se deve ter quando fizer uso das extensões, é na definição da criticidade ou não da extensão. Se uma extensão for definida como sendo crítica, ela pode inviabilizar o campo para uso em um contexto geral.

Segue abaixo algumas extensões pré-definidas:

3.2.2.1.9.1 Identificador de auditoria

Requerido em algumas situações com o objetivo de se realizar auditorias.

Este campo não deve permitir a identificação direta do titular. Para a devida identificação do titular, o sistema auditor deve consultar o emissor do CA, que deve manter mecanismos para a correta identificação do titular.

Esta extensão, se usada, deve ser considerada como crítica.

3.2.2.1.9.2 Identificador do sistema usuário

Esta extensão permite que sejam definidos os serviços autorizados a usar o CA. Caso o serviço não esteja listado nesta extensão, o sistema verificador poderia rejeitar o CA.

Se a extensão não estiver presente, o CA deve ser aceito por qualquer servidor.

Esta extensão contém apenas uma lista com os nomes dos serviços.

Se a extensão estiver presente, o sistema verificador (que seja honesto) deve fazer a verificação se os seus serviços podem ser acessados usando este CA.

3.2.2.1.9.3 Identificador da chave da autoridade de atributo

A extensão authorityKeyIdentifier é usada pelo verificador do CA para checar a assinatura do emissor.

3.2.2.1.9.4 Informação de acesso à autoridade de atributo

A extensão authorityInformationAccess é usado pelo verificador para checar o estado de revogação do CA. A verificação é realizada por meio do protocolo OCSP (MYERS, 1999).

3.2.2.1.9.5 Ponto de acesso à LCAR

A extensão crlDistributionPoints é usado pelo verificador para checar o estado de revogação do CA. A verificação é realizada por meio da LCAR.

3.2.2.1.9.6 Existência mecanismo de revogação

Esta extensão permite ao emissor indicar a inexistência de mecanismos de verificação de revogação. Este mecanismo é usado geralmente quando o tempo de vida do CA é curto.

3.2.3 Fonte de Autoridade de Atributo

A Fonte de Autoridade de Atributo (FAA) é a entidade raiz confiável para a emissão do atributo. A sua principal função é oferecer credibilidade e a validade de uma determinada informação, ou seja, a entidade deve ter a garantia jurídica e a confiança de que é responsável por um determinado atributo.

3.2.4 Autoridade de Atributo

A entidade que detém o poder de conceder um determinado atributo a uma entidade é denominada de Autoridade de Atributo (AA).

3.2.5 Lista de Certificados de Atributos Revogados

Da mesma forma e motivo que existem as LCRs de ICP, existe também a possibilidade de se criar uma Lista de Certificados de Atributos Revogados (LCAR). Esta lista é mantida pelas AAs, nos casos em que exista mecanismo de revogação para um determinado atributo.

Os mecanismos de revogação são desnecessários nos cenários nos quais o período de validade de um CA é menor do que o tempo necessário para emitir e distribuir a informação de revogação. Nesses casos, é melhor revalidar o atributo periodicamente em vez de manter uma estrutura de revogação (ETSI, 2002).

Porém, quando estes certificados de atributos têm uma vida mais longa, é necessário existir uma estrutura de revogação semelhante à existente na ICP para CI.

A informação de que existe ou não uma infraestrutura disponível para a verificação de revogação deve estar explícita no certificado conforme RFC 5280 (COOPER et al, 2008, p.45).

Para a consulta do estado de revogação de um CI pode ser utilizado o OCSP (*Online Certificate Status Protocol*) (MYERS et al, 1999) ou a LCR (Lista de Certificados Revogados) (COOPER et al, 2008).

A possibilidade de usar os mesmos mecanismos de revogação dos CIs (OCSP e LCR) para os CAs é descrita na RFC 5755 (FARRELL et al, 2010).

3.3 Tipos de atributos

A RFC 5755 (FARRELL et al, 2010) define alguns tipos de atributos que um CA pode conter:

a) Informação de serviço de autenticação;

b) Identificação de acesso;

c) Identificação de Cobrança;

d) Grupo;

e) Papel;

f) Nível de acesso.

3.3.1 Informação de serviço de autenticação

O CA pode conter um tipo de atributo usado para efetuar autenticação (*Service Authentication Information*) (FARRELL et al, 2010, p.20).

Geralmente, este atributo contém o par usuário/senha para aplicações legadas. Estas informações serão criptografadas caso possuam informações sensíveis (uma senha, por exemplo). Nem sempre o portador do CA deseja que o atributo seja visto por qualquer sistema. Nestas situações além da identificação do sistema alvo, o atributo deve ser criptografado (LINN, 1999, p.123).

3.3.2 Identificação de acesso

O CA pode conter um tipo de atributo usado para efetuar identificação de acesso (*Access Identity*) (FARRELL et al, 2010, p.21).

O objetivo deste atributo é prover informações sobre o titular do CA, que pode ser usado pelo sistema verificador de privilégios para autorizar determinadas ações do titular dentro do sistema.

3.3.3 Identificação de cobrança

O CA pode conter um tipo de atributo usado para fins de cobrança (*Charging Identity*) (FARRELL et al, 2010, p.22).

O objetivo deste atributo é prover informações para o propósito de cobrança. Geralmente o identificador de cobrança será diferente de outros identificadores do titular. Como exemplo, o nome da empresa onde trabalha o titular, será a entidade responsável pelo pagamento de um serviço.

3.3.4 Grupo

O CA pode conter um tipo de atributo usado para definir que o portador pertence a um determinado grupo (*Group*) (FARRELL et al, 2010, p.22).

Este tipo de atributo é bastante útil e comum e é apresentado como uma das classes de aplicabilidade na seção 3.4.1.

3.3.5 Papel

O CA pode conter um tipo de atributo usado para definir o papel que o portador desempenha (*Role*) (FARRELL et al, 2010, p.22).

Este tipo de atributo é bastante útil e comum e é apresentado como uma das classes de aplicabilidade na seção 3.4.3.

3.3.6 Nível de acesso

Este atributo contém informações relativas ao nível de acesso do titular do CA (*Clearance*) (FARRELL et al, 2010, p.23).

Pode ser usado para identificar a política de segurança à qual o nível de acesso está relacionado. Existem 6 níveis de acesso reservados e pré-definidos: sem definição, irrestrito, restrito, confidencial, secreto e altamente secreto. Além destes níveis de acesso, as organizações podem criar as suas próprias políticas de acesso.

A utilidade deste tipo de atributo é média, pois geralmente, a definição do nível de acesso é realizada pelo próprio sistema verificador de privilégios que se baseia nas credenciais apresentadas pelo usuário.

3.4 Classes de aplicabilidade

Os CAs podem ser usados para diversas finalidades. Os principais usos são: a vinculação do portador a uma determinada entidade, a atribuição de um estado, propriedade ou situação atual ao portador, a atribuição de um papel ou função ao portador do certificado e na delegação de tarefas (FARRELL et al, 2010).

3.4.1 Vínculo a uma entidade

Neste tipo de aplicação, o CA é usado para informar que o portador é vinculado a alguma entidade. Neste caso, a informação do vínculo existente entre o portador e a entidade pode ser usada na definição do nível de acesso ao qual o portador tem direito. Um exemplo deste tipo de aplicação pode ser a designação de que uma determinada pessoa é integrante do colegiado de advogados inscritos na entidade OAB.

3.4.2 Atribuição de estado

O CA pode ser usado para atribuir um determinado estado ou situação atual do portador. Neste caso a Autoridade de Atributo, emite o certificado indicando que, naquele momento, o portador encontra-se em uma determinada situação. As aplicações deste tipo de certificado, geralmente têm um prazo de validade curto (geralmente alguns dias), pois a situação do usuário pode mudar com certa freqüência. Este tipo de certificado pode ser adotado, por exemplo, nos cartórios para fornecer um comprovante da condição civil de uma pessoa.

3.4.3 Atribuição de papel

A outra forma de uso dos certificados de atributos seria na atribuição de um papel ou função. A atribuição de uma função ao portador pode ser usada para a definição dos níveis de privilégios que o portador tem para acessar um sistema. Um sistema de segurança pode atribuir níveis de acesso a um local, baseado na função das pessoas. Um CA que determina a função do titular pode ser usado por esse sistema na definição dos privilégios de acesso. Exemplo: um gerente de loja pode autorizar um desconto. Se um indivíduo possuir o atributo “gerente de loja”, automaticamente, o sistema pode liberar uma tela para autorizar o desconto.

3.4.4 Delegação de tarefas

O uso de credenciais na delegação de tarefas com CI é uma técnica descrita na RFC 3820 (TUECKE et al, 2004). Esta técnica pode ser usada nos sistemas de segurança para permitir que uma entidade dê permissão para outra entidade atuar como sendo a primeira. Este tipo de aplicação pode ser muito útil, pois nem sempre a entidade autorizada a executar determinada tarefa está disponível para executá-la.

O uso dos certificados de atributos em delegação de tarefas pode ir mais além do que apenas permitir que uma entidade aja em nome de outra. Ele pode ser usado também para restringir o tipo de tarefa ao qual está sendo autorizado ou restringir o sistema alvo para o qual o CA foi emitido (LINN, 1999). Pode-se, por exemplo, definir que a delegação de uma tarefa permita apenas a leitura de dados de um determinado sistema. Isto transforma a delegação de tarefa do tipo “agir em nome de” para “agir em nome de, desde que apenas leia os dados, sem poder alterá-los”, ampliando significativamente os níveis de segurança desta operação.

3.5 Certificado de Atributo na Delegação de Tarefas

Existem cenários em que o mecanismo de delegação de privilégio é algo desejável. Estas situações ocorrem quando é necessário que uma entidade possa realizar tarefas por meio de autorização fornecidas por outra entidade detentora do privilégio.

Uma das formas de uso dos CA é permitir realizar a delegação de permissões. Neste tipo de aplicação, a fonte de autoridade é a primeira emissora de certificados que atribuem privilégios aos titulares. Um dos privilégios concedidos pela fonte de autoridade pode ser a permissão de delegar os privilégios a outra entidade. Com esta autorização, o titular do privilégio, pode atuar como uma AA e delegar o seu privilégio a outras entidades por meio da emissão de um CA que contenha o mesmo privilégio (ou um subconjunto dele). A fonte de autoridade pode impor algumas restrições sobre delegação, como, por exemplo, limitar o comprimento máximo da cadeia de delegação, limitar os nomes dos titulares permitidos para receber aquele privilégio e outros.

Cada uma das AAs intermediárias pode delegar, no máximo, os seus próprios privilégios, não sendo possível delegar mais privilégios do que aqueles detidos por elas.

Quando a delegação é usada, o sistema verificador de privilégios confia na fonte de autoridade para delegar todos ou alguns de seus privilégios para os titulares, os quais ainda podem delegar todos ou alguns de seus privilégios a outros titulares.

O verificador de privilégios confia que a fonte de autoridade tem a autoridade de um determinado conjunto de privilégios para acesso ao recurso. Se o privilégio definido no CA não tiver sido emitido pela fonte de autoridade, o verificador de privilégios deve verificar a cadeia de delegação até encontrar o privilégio emitido pela fonte de autoridade. A validação da delegação inclui a verificação de todas as AAs da cadeia de delegação, inclusive verificando se cada uma delas possui os privilégios suficientes e se havia a autorização para delegar os privilégios.

Segundo CHADWICK (2002) são pré-requisitos para a delegação de privilégios:

a) CAs emitidos para entidades finais devem ser diferentes dos CAs emitidos pela AA. O objetivo é evitar que uma entidade final consiga estabelecer a ela mesma uma AA sem autorização. É necessário também que uma AA possa determinar a profundidade das delegações subseqüentes que serão permitidas;

b) dentro do âmbito da delegação, uma AA deve ser usar um nome de forma que um sistema verificador de privilégios seja capaz de verificá-lo;

c) uma AA precisa ser capaz de especificar uma política de certificados (de chave pública) aceitos no processo de autenticação de todos os titulares presentes na cadeia de delegação;

d) um sistema verificador de privilégios deve ser capaz de localizar o CA correspondente para checar se o emissor tinha privilégio suficientes para delegar privilégios no certificado.

3.5.1 Extensões de Delegação

Os seguintes campos foram definidos em extensões para suportar a delegação de tarefas por meio dos certificados de atributos (ITU-T, 2000):

a) *Basic attribute constraints*;

b) *Delegated name constraints*;

c) *Acceptable certificate policies*;

d) *Authority attribute identifier*.

3.5.1.1 *Basic attribute constraints*

A extensão "*basic attribute constraints*" é um campo lógico que indica se o titular do CA tem a autorização para delegar privilégio. Se for VERDADEIRO (caso em que é permitido a delegação), o titular pode passar a exercer o papel de uma AA e delegar os seus privilégios. Nesta situação, o campo vem acompanhado de um número inteiro (*pathLenConstraint*) que indica o número de vezes que a delegação será permitida. O valor 0 (zero) significa que a AA pode emitir CA apenas para entidades finais e não para AA (nenhuma delegação é permitida). O valor 1 (um) significa que o titular de um privilégio também pode exercer o papel de AA e delegar os seus privilégios mais uma vez apenas. Incrementar este campo corresponde aumentar o número de delegações que podem ocorrer da cadeia de delegação.

Se o campo *pathLenConstraint* não for definido, significa que não há limite para o tamanho da cadeia de delegação. Note-se que a restrição tem efeito a partir do próximo CA da cadeia. O campo *pathLenConstraint* controla o número de certificados entre o CA da AA e o CA da entidade final.

Esta extensão pode, a critério do emissor, ser considerada crítica ou não crítica. A recomendação é que seja definida como crítica (ITU-T, 2000). Do contrário, um titular não autorizado a ser uma AA pode emitir um CA e o sistema verificador pode inadvertidamente usar este CA.

Caso a extensão esteja presente e definida como crítica, então:

a) se o valor do campo estiver FALSO, então a delegação não será usada;

b) se o valor do campo estiver VERDADEIRO e o campo “*pathLenConstraint*” existir, então o verificador de privilégios deve checar se a cadeia de delegação está consistente com o valor o campo “pathLenConstraint”.

Caso a extensão esteja presente, definida como não crítica e não for reconhecida por um sistema verificador, então o sistema deve usar outros meios de determinar se o atributo pode ser usado para delegação.

Se a extensão não estiver presente, ou se a extensão estiver presente com o campo vazio, então o titular será limitado a ser apenas uma entidade final, não sendo permitida qualquer delegação de privilégios.

3.5.1.2 *Delegated name constraints*

A extensão “*delegated name constraints*” permite a AA restringir os nomes dos titulares a quem os privilégios podem ser delegados. O campo é composto por nomes permitidos e/ou por nomes não permitidos (*permited subtrees or excluded subtrees*), ou seja, o nome do titular deve estar listado nos nomes permitidos ou não estar na lista de nomes excluídos.

Se ambos “*permittedSubtrees*” e “*excludedSubtrees*” estiverem presentes e um determinado nome estiver presente em ambos, a exclusão terá precedência (ITU-T, 2000).

Esta extensão pode ou não ser definida como crítica a critério do emissor. Porém é recomendável que seja definida como crítica, pois, do contrário, um sistema usuário de um CA pode não verificar nos subseqüentes CA da cadeia de delegação se o titular está listado dentre os nomes destinados pela AA emissora.

3.5.1.3 *Acceptable (public key) certificate policies*

A extensão “*acceptable certificate policies*” é usada para garantir que o CA emitido pelo titular dos privilégios esteja vinculada a um certificado de identidade emitido sob uma política aceitável de certificação. Isto é usado para garantir que o titular do CA tenha sido autenticado por um CI e uma chave pública com um nível de confiança

necessário, fazendo com que o processo de delegação não seja comprometido pelo uso de uma política de certificação fraca do processo de autenticação.

Esta extensão deve estar presente apenas nos CAs emitidos para uma AA. Esta extensão não deve ser incluída nos CAs da entidade final.

Se presente, esta extensão deve ser definida como crítica.

Se esta extensão estiver presente e o verificador de privilégios reconhecê-la, o verificador deve verificar se todos os titulares dos privilégios subseqüentes da cadeia de delegação foram autenticados por uma chave pública emitida sob uma das políticas listadas.

Caso esta extensão esteja presente, mas não compreendida pelo verificador de privilégios, o certificado deve ser rejeitado.

3.5.1.4 *Authority attribute identifier*

A extensão "*authority attribute identifier*" é um ponteiro que remete de volta para o CA da AA. Isso permite que o verificador de privilégios analise se os privilégios da AA são suficientes para conceder a delegação de privilégios no CA corrente. Seguindo toda a cadeia inversa dos certificados, o sistema verificador deve chegar a um CA emitido por uma fonte de autoridade confiável, situação no qual o acesso ao recurso será concedido.

Na delegação de privilégios, uma AA deve ter pelo menos o mesmo privilégio concedido, assim como a autoridade de delegar aquele privilégio. Uma AA que está delegando um privilégio para outra AA ou para uma entidade final, deve informar esta extensão no CA que está emitindo.

Um CA que contém esta extensão pode incluir a delegação de múltiplos privilégios para o titular do certificado. Se a concessão desses privilégios tiver sido feita para mais do que um certificado, então esta extensão deve incluir mais de um ponteiro.

Esta extensão é sempre definida como não crítica.

3.6 Vínculo entre o CA e o CI

Uma das questões que envolvem o uso dos certificados de atributos está relacionada à forma como ele será vinculado ao CI. Segundo PARK (2000) existem três formatos de vínculos que podem ser adotados: monolíticas, autônomas ou em cadeia. Cada formato tem as suas próprias características, vantagens e desvantagens, podendo também ser gerados modelos híbridos. PARK (2000) chama cada um destas formas de vínculo de “assinatura” e nesta dissertação o termo foi substituído por “estrutura”.

3.6.1 Estrutura Monolíticas

Esta forma de vínculo é usada quando existe apenas uma autoridade que controla a identidade e os atributos do titular, esta autoridade está apta a assinar os dois conjuntos de informações em um único certificado. Uma vez que a identidade e os atributos estão no mesmo certificado com uma única assinatura da autoridade certificadora, qualquer alteração que ocorra, seja ela na identificação ou nos atributos do titular, o certificado deverá ser reemitido.

A vantagem deste perfil é a simplicidade no gerenciamento, uma vez que todas as informações necessárias à aplicação estão em um único certificado, bastando apenas, para verificar a autenticidade e validade, checar a assinatura da autoridade certificadora, sua cadeia de certificação e a lista de certificados revogados.

Entretanto, este formato não é adequado quando a autoridade certificadora e a fonte de autoridade de atributo são distintas. Quando existirem atributos ou identificações, os quais são controlados por diferentes autoridades, provendo diferentes períodos de validade para cada informação, o formato monolítico não pode ser usado. É um método simples, porém reduz a flexibilidade (Figura 4).

É o método utilizado atualmente pela RFB no e-CPF, no qual a AC-RFB possui a prerrogativa legal de emitir o CI da ICP-Brasil e o atributo CPF. Este método não é recomendado, pois informações de autorização geralmente não têm o mesmo tempo de vida que o vínculo entre a identidade e a chave pública. Além disso, o emissor

do CI geralmente não está autorizado a definir as informações de autorização (FARRELL et al, 2010, p.3).

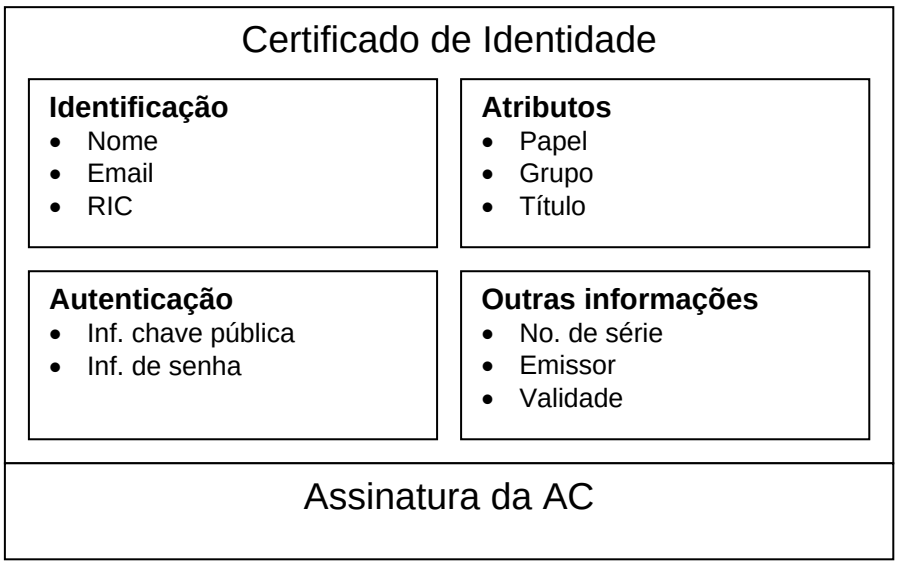

Figura 4 - Estrutura Monolítica

Fonte: elaborado pelo autor e adaptado de PARK (2000)

3.6.2 Estruturas Autônomas

Esta forma de vínculo suporta várias autoridades certificadoras e conseqüentemente, diferentes validades para os CIs e os CAs. Uma pessoa poderia ter vários CIs, emitidos por CAs distintas. Estes CIs não possuem nenhum atributo do titular, mas apenas a sua identificação. Na seqüência, é emitido um CA ao titular do CI por uma AA. Nesta situação, o campo usado para fazer o vínculo entre os certificados é um campo único de identificação do titular. Segundo PARK (2000) é possível também usar outros campos para fazer este vínculo, como a chave pública do titular (campo *Subject* do CI e campo *Holder* do CA), o resumo da chave pública, a senha criptografada, o resumo da senha ou o número serial do CI e o emissor. Entretanto, se forem usados estes campos, não estará aderente à especificação da RFC 5755 e o CA ficará vinculado ao CI correspondente, perdendo a sua

flexibilidade de uso. O critério de escolha do campo é definido pela própria aplicação usuária.

A vantagem deste método é obtida quando o campo vinculante utilizado é um identificador do titular e não do certificado. Assim todos os demais campos do CI podem ser alterados sem invalidar o CA. A outra vantagem pode ser observada quando, por exemplo, existam dois CIs diferentes, mas que possuem o mesmo campo usado para vincular um CA. Qualquer um dos CIs poderia ser usado para prover a autenticação do usuário.

Existe mais uma vantagem deste formato: como pode ser usado um campo identificador qualquer do portador, o CA fica vinculado ao titular e não ao CI. Algumas aplicações que não necessitam de mecanismos de autenticação podem fazer uso deste tipo de CA. Um exemplo deste uso é apresentado na seção 7.1.

Este tipo de estrutura é previsto na RFC 5755, quando se usa a opção *entityName* no campo *Holder* (FARRELL et al, 2010, p.12).

As vantagens deste perfil são a flexibilidade e reuso dos certificados (Figura 5).

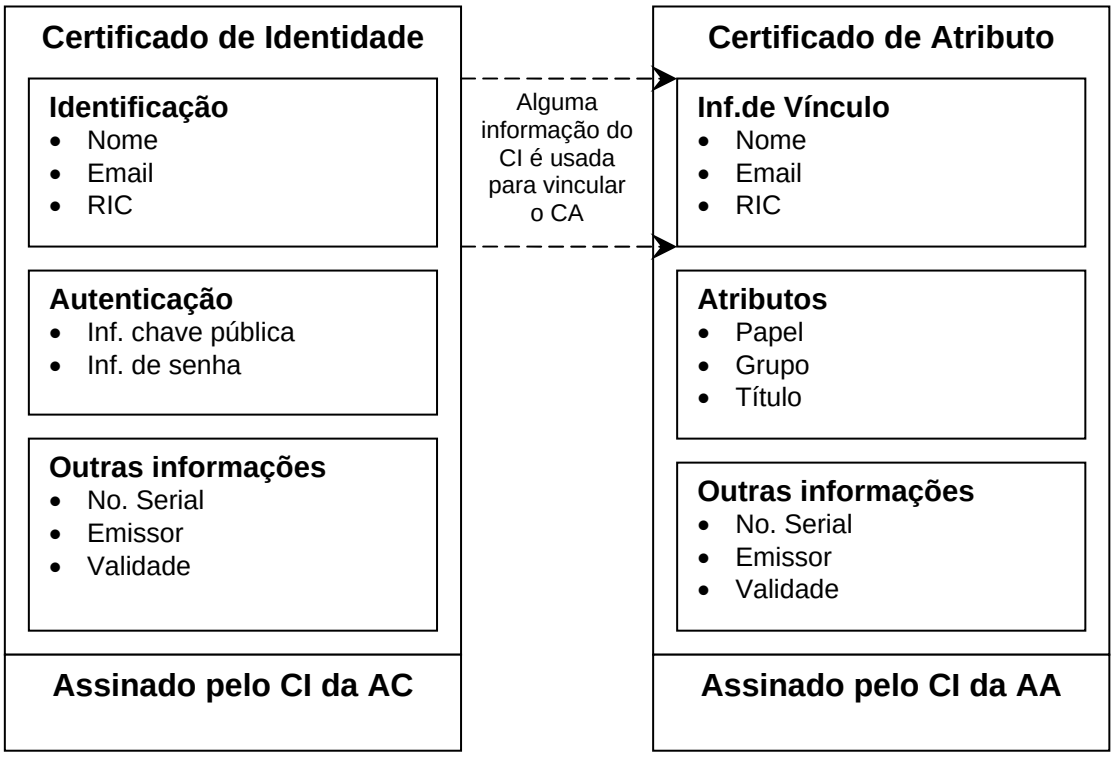

Figura 5 - Estruturas Autônomas

Fonte: elaborado pelo autor e adaptado de PARK (2000)

3.6.3 Estruturas em Cadeia

Esta forma de vínculo suporta múltiplas AAs e diferentes validades para CI e CA mas, diferentemente da estrutura autônoma, este perfil estabelece uma forte ligação entre o CI e o CA.

Para ilustrar esta forma de vínculo, uma pessoa tem um ou mais CIs emitidos assinados digitalmente por diferentes ACs, como ocorre normalmente. Na seqüência, uma AA emite um CA para o titular, vinculando o CA a um dos seus CIs. Vários CAs podem ser emitidos por diferentes AAs para o mesmo ou diferentes CIs da pessoa.

Neste perfil, o vínculo é feito pela assinatura digital da AC do CI do titular, de forma que a expiração, a revogação ou qualquer alteração na informação do CI que causa a renovação do CI invalida também os CAs, aos quais o CI estão associados (Figura 6).

Este tipo de estrutura é previsto na RFC 5755 quando se usa a opção *ObjectDigestInfo* no campo *Holder* (FARRELL et al, 2010, p.31).

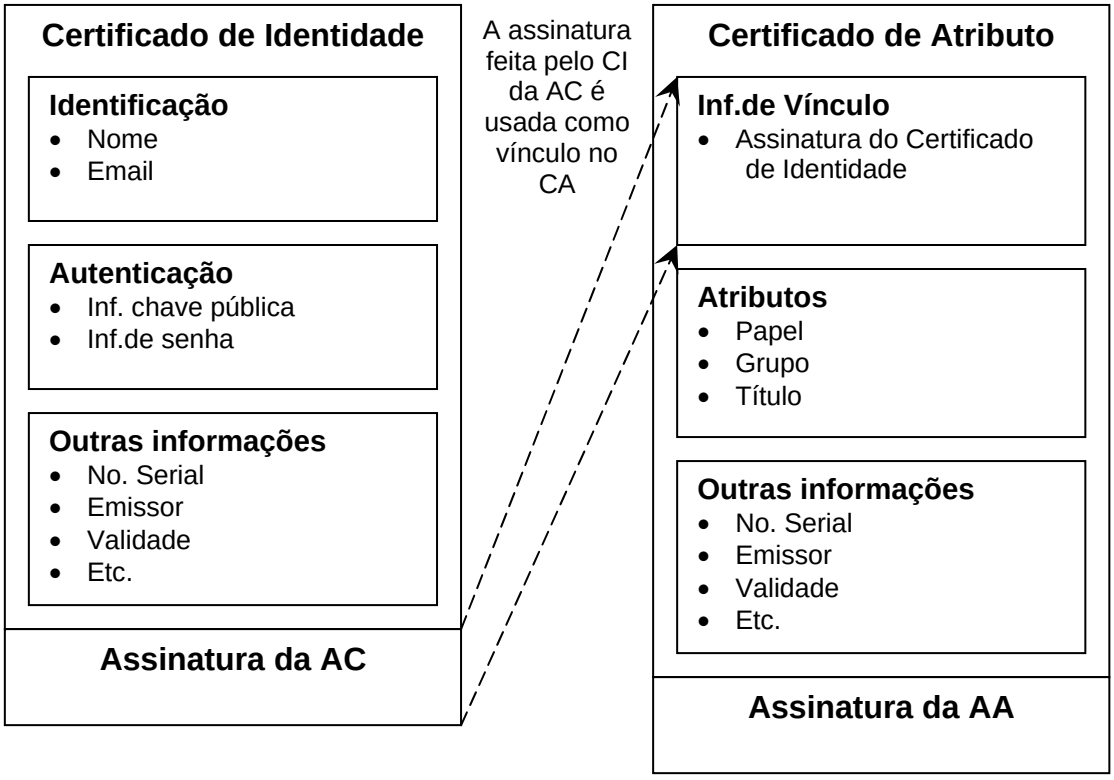

Figura 6 - Estrutura em Cadeia

Fonte: elaborado pelo autor e adaptado de PARK (2000)

3.6.4 Análise dos tipos de vínculo entre CI e CA.

Pelas características de cada tipo de vínculo entre CI e CA, observa-se que a escolha de um tipo ou de outro vai depender principalmente do tipo da aplicação.

A estrutura monolítica é o mecanismo mais simples, porém exige-se que os atributos e o CI tenham o mesmo período de validade e mesma fonte de autoridade de atributo. Tecnicamente falando, a identidade e os atributos com diferentes períodos de validade, podem ser armazenados em um único certificado emitido pela AC. No entanto, nesta situação, quando uma determinada informação (geralmente um atributo) deve ser renovada ou revogada, torna-se necessária a renovação ou

revogação de todo o certificado, incluindo os dados de identificação e os demais atributos que porventura fizerem parte do certificado.

Por outro lado, a estrutura autônoma e a estrutura em cadeia permitem a renovação ou revogação dos CAs de forma independente. Portanto, se a aplicação necessita de diferentes períodos de validade entre atributos e dados de identificação, ou as AAs são entidades diferentes das ACs, deve-se adotar a estrutura autônoma ou em cadeia.

A estrutura monolítica e em cadeia fornecem um mecanismo bastante forte de vínculo com o CI, de forma que, se qualquer informação do CI for alterada, o vínculo com o CA será quebrado. Na estrutura autônoma este vínculo é mais flexível, pois se podem alterar alguns dados do CI, sem que o CA perca o seu respectivo vínculo.

O mecanismo de verificação da correspondência com o CI não é necessária quando os atributos e os dados de identificação estão armazenados em uma única credencial. Portanto a estrutura monolítica é um perfil de fácil verificação. No entanto, tem baixa capacidade de reutilização de certificados, porque qualquer alteração nos atributos ou no certificado exigirá a emissão de um novo certificado. Diferentemente das estruturas autônomas ou em cadeia, nos quais a verificação da correspondência ao CI é relativamente difícil, pois cada CA não está necessariamente vinculado a um determinado CI.

A estrutura autônoma suporta alta reusabilidade, porque o CI ou o CA podem ser alterados sem que ocorra um rompimento da ligação entre eles, desde que o campo vinculante se mantenha o mesmo. A contrapartida é a dificuldade para descobrir o CI correspondente, pois poderão existir vários CIs aptos a serem aceitos e o campo vinculante usado deve ser bem determinado. O que não ocorre com as estruturas monolíticas e em cadeia, pois o CI correspondente é sempre determinado.

A Tabela 2 apresenta um comparativo das 3 formas de estruturas com o a análise dos seguintes itens:

a) CAs – quantidades de CAs que podem ser emitidos para um CI;

b) Validade – a validade dos CAs e o CI;

c) Vínculo do CA com CI – a força do vínculo entre o CA e o CI;

d) Reuso – a capacidade de reuso dos CAs quando ocorre uma alteração no CI.

Tabela 2 - Comparativo entre as formas de estruturas do CA

Item analisado	Monolítica	Autônoma	Em Cadeia
CAs	Único	Vários	Vários
Validade	Única	Diferentes	Diferentes
Vínculo do CA com o CI	Forte	Fraco	Forte
Reuso	Baixo	Alto	Médio

Fonte: elaborado pelo autor e adaptado de PARK (2000)

4 OS CERTIFICADOS DE ATRIBUTO E O CERTIFICADO DE IDENTIDADE NA ICP-BRASIL

Nesta seção será apresentada a análise da utilização de atributos no âmbito da ICP-Brasil.

4.1 ICP Brasil

Segundo a própria definição da ICP-Brasil ela “é um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras, com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública” (ICP-BRASIL, 2007).

A ICP-Brasil foi instituída pela Medida Provisória 2.200/2001 e as atividades do Comitê Gestor foram regulamentadas e definidas pelo decreto 3.872/2001. O Comitê Gestor é o órgão governamental que tem por função adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil.

Além disso, o comitê tem ainda as seguintes funções (BRASIL, 2001):

a) estabelecer a política de certificação e as regras operacionais da AC Raiz, além de homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

b) estabelecer as diretrizes e normas para a formulação de políticas de certificados e regras operacionais das ACs e das Autoridades de Registro (ARs) e definir níveis da cadeia de certificação.

c) aprovar as políticas de certificados e regras operacionais, licenciar e autorizar o funcionamento das ACs e das ARs, bem como autorizar a AC Raiz a emitir o correspondente certificado, identificar e avaliar as políticas de ICP externas, quando for o caso, certificar sua compatibilidade com a ICP-Brasil, negociar e aprovar, observados os tratados, acordos e atos internacionais, acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional e ainda, atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua

compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

A AC Raiz é a primeira autoridade da cadeia de certificação. É a executora das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor.

O ITI – Instituto Nacional de Tecnologia da Informação opera a AC-Raiz da ICP-Brasil (art. 13 MP 2.200/2001). As suas atribuições têm características próprias das agências reguladoras, pois têm o poder de direcionar as atividades dos fornecedores privados de chaves de assinatura e certificados digitais, de acordo com interesses públicos juridicamente definidos. Embora o ITI e o Comitê Gestor da ICP-Brasil não tenham recebido a denominação de “órgão regulador” ou “agência reguladora” nos textos normativos referentes à atividade de certificação digital, ou mesmo em qualquer outro documento legal, na prática funcionam com poderes próprios desses órgãos (REINALDO, 2006).

Qualquer organização ou empresa pode criar sua própria AC e, dependendo de requisitos técnicos e legais de operabilidade, podem requerer registro junto à ICP-Brasil. Se uma AC criada e mantida por uma instituição qualquer se adequar às práticas de certificação aos regulamentos gerais da ICP-Brasil, pode vir a fazer parte de sua infraestrutura, passando a ser mais um membro da cadeia nacional de confiança, ampliando assim o poder de validade de seus certificados. Uma AC credenciada à ICP-Brasil pode vender certificados que sirvam para verificar assinatura em qualquer tipo de documento ou transação, com validade jurídica em todo o território nacional.

Atualmente, a ICP-Brasil tem 9 ACs de primeiro nível e 27 ACs de segundo nível (base Junho de 2010).

4.2 Análise de vínculo entre o CA e atributos

O uso da estrutura monolítica, apresentada na seção 3.6.1, é a forma utilizada atualmente pelo CI e-CPF. A vantagem deste perfil é que ele é de simples

administração. Entretanto, ela não é a mais adequada se comparada com a estrutura autônoma.

Na ICP-Brasil, existe uma proposta (SERASA, 2007) de atributos com o uso de estrutura autônoma, (seção 3.6.2), ou seja, seria usado um dos campos do CI (por exemplo, o no. do RG) para fazer o vínculo com o CA. A idéia defendida por este trabalho é que o atributo pertence à pessoa e não ao certificado digital, cuja função é apenas identificar o titular.

Um problema apontado por esta proposta reside no fato que os campos dos certificados da ICP-Brasil são compostos por várias informações (RG, CPF, Título de Eleitor, etc.). Isto contraria a padronização, uma vez que o padrão considera que o vínculo entre o CI e o CA deve ser realizado por um identificador único. Haveria, então, a necessidade da criação deste identificador único do titular, que seria colocado no campo "*Subject*" ou na extensão "*Subject Alternative Name*", o qual faria a ponte de ligação do CI e todos os CAs do titular.

A estrutura em cadeia somente seria adequada nas situações em que fosse necessária uma forte ligação entre o CI e o CA. Nestes casos quando o CI expira ou é revogado, automaticamente todos os CAs a ele vinculados também perdem automaticamente a validade, uma vez que o vínculo é quebrado. Um exemplo hipotético poderia ser o próprio CPF, que poderia ser eliminado do CI e transformado em um CA. Os dois certificados estariam vinculados por uma estrutura em cadeia, ou seja, por meio da assinatura da AC presente no CI. Caso o CI fosse expirado ou revogado, automaticamente o CA de CPF também seria.

4.3 Uso do Registro de Identidade Civil (RIC) como campo vinculante entre os CAs e a Pessoa Física

Conforme apresentado na seção 3.6.2, a forma mais adequada de vínculo entre o CA e a entidade é realizada usando-se um campo de identificação da entidade.

Entretanto para que exista a possibilidade não apenas vincular o CA à entidade, mas também a um CI da entidade é necessário que o campo para "*Holder.entityName*"

seja codificado com o conteúdo do campo “*Distinguished Name*” do CI (FARRELL et al 2010, p.34).

O desafio passa a ser então encontrar o conteúdo ideal para o preenchimento do campo vinculante “*Distinguished Name*”, pois desta forma os CAs poderiam funcionar em conjunto ou não com os CIs.

A Lei no. 9.454 de 7 de Abril de 1997 instituiu o número único de Registro de Identidade Civil (RIC) e no seu artigo 2º definiu a criação de uma Cadastro Nacional de Registro de Identificação Civil.

Em Julho de 2008, durante o Encontro Nacional de Identificação realizado em Brasília, foi anunciado que finalmente ela será implantada com a conclusão total prevista para 2017.

Ao longo do ano de 2009, várias discussões estiveram em curso no Congresso Nacional na tentativa de regulamentar e viabilizar a implantação do RIC no país.

Finalmente em Maio de 2010 por meio do Decreto do Executivo Federal No. 7.166/2010 ocorreu a criação do sistema nacional de registro de identificação civil, instituiu o seu comitê gestor e regulamentou as disposições da Lei no. 9.454. Com isto, em breve teremos o RIC à disposição.

Caso o RIC não viesse a existir, a alternativa seria o campo Registro Geral (RG) emitido pelas Secretarias de Segurança Pública dos estados da federação.

Como o RIC é um ótimo campo para a identificação das pessoas e tendo em vista a sua aprovação, este campo é considerado neste trabalho como o principal campo vinculante entre os certificados digitais (CI e CA) e o cidadão, embora não tenha sido realizada uma definição clara de todo o conteúdo deste “*Distinguished Name*” sugerido.

4.4 Segurança da IGP

A segurança nos processos de autenticação e autorização é um dos motivos da adoção dos certificados digitais. A seguir são listadas algumas considerações de

segurança que devem ser observadas conforme a RFC 5755 (FARRELL et al, 2010):

a) para os certificados de identidade, a proteção das chaves privadas é um fator crítico para a manutenção da segurança. Uma falha na AA na proteção da sua chave privada permitirá que um atacante possa se passar como sendo a própria AA, podendo gerar falsos CAs ou falsas listas de revogação, o que acarretaria em perda da confiança do sistema. Caso isto ocorra, todos os CAs emitidos pela AA devem ser revogados. A reconstrução é bastante problemática, sendo, portanto um importante ponto de vulnerabilidade e que deve ser bastante protegido por meio de mecanismos fortes de segurança (uso de equipamentos criptográficos à prova de violações, gestão de procedimentos seguros, etc.), para evitar a sua ocorrência;

b) a perda da chave privada pela AA, também é bastante problemática, pois a AA não seria capaz de gerar uma revogação ou executar uma renovação de um CA. As AAs são aconselhadas a manter cópias de segurança para evitar a perda da chave privada.

c) outro aspecto que afeta a segurança do CA é o seu tempo de vida. AA que emite CA de longa duração deve disponibilizar mecanismos de revogação, pois durante a vida do CA podem ocorrer eventos que eliminem ou alterem o atributo do titular. Caso os mecanismos de revogação não estejam disponíveis para consulta, a confiabilidade do CA será reduzida;

d) tamanho de chaves curtas ou algoritmos criptográficos fracos também podem ser pontos de vulnerabilidade. As AAs devem sempre usar as recomendações de algorítmos criptográficos;

e) as aplicações que farão uso dos CAs devem usar as regras padronizadas definidas pela recomendação X.500 para a comparação dos nomes únicos (*Distinguished Names*). A inconsistência na comparação pode resultar em aceitação de credenciais inválidas ou a rejeição de credenciais válidas;

f) as AAs devem codificar o nome único no campo *holder.entityName* do CA igual ao campo *Distinguished Name* do CI. Se forem usadas codificações

distintas, as aplicações podem não reconhecer que um CA e um CI pertencem à mesma entidade.

4.5 Validade legal e regulamentação

Na prática já existe embasamento legal para o uso dos CAs. Uma vez que as assinaturas eletrônicas são reconhecidas por lei (BRASIL, 2001) e o CA sendo um documento assinado digitalmente, não existe restrição legal para a sua adoção. Ou seja, desde que o CA seja assinado por meio de um CI da ICP-Brasil, ele está dentro da legislação atual e deve ser aceito pelas entidades. Porém, não existe regulamentação técnica a respeito do uso de CA no âmbito da ICP-Brasil.

5 ESTUDOS DE CASOS

Na seleção dos estudos de casos, procurou-se por processos relevantes para o contexto dos CAs, bem como a possibilidade de estudar de forma abrangente as situações mais comuns de uso dos CAs.

Assim, foram selecionados os seguintes casos:

a) Certificação Digital da OAB;

b) Cadastro de Pessoa Física – CPF;

   - ✓ consulta nome e situação cadastral;
   - ✓ atendimento eletrônico da Pessoa Física;

c) e-CNPJ;

d) Prontuário Eletrônico de Paciente (PEP).

O estudo de caso “Certificação Digital da OAB” foi escolhido porque é um cenário:

a) em funcionamento na vida real no qual os CIs têm sido usados para efetuar não apenas a identificação da pessoa, mas também para atribuir a qualidade de advogado ao portador;

b) muito semelhante ao cenário em uso na Espanha pelo ICAM (equivalente à OAB) por meio dos CAs;

c) que possui alto potencial de uso, pois poderia ser utilizada na prática por qualquer entidade de classe;

d) no qual é possível descrever a funcionalidade do atributo “grupo” padronizado em FARRELL et al (2010).

A aplicação “consulta nome e situação cadastral” do estudo de caso “Cadastro de Pessoa Física - CPF” foi escolhida porque se trata de uma aplicação:

a) em funcionamento na site da RFB que possui alto potencial de uso e benefício;

b) no qual é usado CA sem a necessidade de CI, ilustrando que um CA não necessariamente está vinculado a um CI;

c) no qual são analisados os métodos de emissão dos CAs, se por “*push*” ou “*pull*”, além de expor o funcionamento dos mecanismos de revogação dos CAs e as variáveis que devem ser observadas para a existência ou não desses mecanismos;

d) que descreve a funcionalidade de atribuição de estado que pode ser obtido com o uso de CAs.

As razões que levaram a aplicação “atendimento eletrônico da Pessoa Física” do estudo de caso “Cadastro de Pessoa Física - CPF” ser escolhida foram:

a) é uma aplicação que usa atualmente o e-CPF que é um tipo de CI de âmbito da ICP-Brasil e emitido sob a árvore de certificação da AC-RFB. Este CI é usado nos sistemas com o objetivo de efetuar uma autenticação segura, bem como também atribuir privilégios baseado no fato do portador se contribuinte da RFB;

b) a possibilidade de ilustrar as vantagens obtidas com relação ao aumento do probabilidade de não revogação dos certificados digitais, além da facilidade de administração de atributos quando ocorre a separação em certificados distintos para a IGP e para a ICP.

A escolha do estudo de caso “e-CNPJ” foi motivada por apresentar as seguintes características:

a) o e-CNPJ é um tipo de CI de Pessoa Jurídica (PJ) de âmbito da ICP-Brasil e emitido sob a árvore de certificação da AC-RFB. Este certificado é muito utilizado pelas empresas na atualidade e, portanto é um importante objeto de estudo uma vez que a proposta trata sobre a aplicabilidade dos CAs no âmbito da ICP-Brasil;

b) o estudo do e-CNPJ avalia o perfil atual do certificado e analisa as adaptações necessárias para que possibilite a interoperabilidade com os CAs;

c) a possibilidade de descrever como os CAs podem ser utilizados nas diversas relações às quais uma empresa está sujeita ao longo da sua vida. Este tipo de aplicação tem um alto potencial de uso, pois são inúmeras as suas possibilidades de uso;

d) os CAs podem ser usados para a definição de papéis que uma determinada pessoa física exerce dentro da pessoa jurídica e desta forma estudar a funcionalidade do atributo “papel” padronizado em FARRELL et al (2010).

A escolha do estudo de caso “Prontuário Eletrônico de Paciente (PEP)” baseou-se por apresentar as seguintes características:

a) ser emblemática na medida em que possui características tipicamente distribuída. Ocorre interação entre sistemas heterogêneos, os usuários podem assumir múltiplos papéis com diferentes fontes de autoridade e por tratar com informações altamente sensíveis é necessário um elevado grau de segurança para o acesso a estas informações;

b) possibilidade de ilustrar o funcionamento dos mecanismos de delegação, embora não se recomende cadeias de delegação (FARRELL et al, 2010);

c) estudar os desafios necessários para a criação de uma padronização dos atributos e dos CAs;

d) discutir a necessidade de regulamentação das fontes de autoridade de atributo.

As seções a seguir detalham cada um destes casos.

6 ESTUDO DE CASO: CERTIFICAÇÃO DIGITAL DA OAB

Este estudo de caso discute sobre a possibilidade da adoção dos Certificados de Atributos pela Ordem dos Advogados do Brasil (OAB) como uma alternativa ao atual sistema na concessão de certificados digitais aos seus advogados inscritos.

6.1 Introdução

Uma das formas de uso da tecnologia de CA é na atribuição de vínculo a entidades de classe (descritas na seção 3.4.1).

No Brasil, a Ordem dos Advogados do Brasil é a entidade de classe que tem a prerrogativa de conceder a carteira da OAB para designar um advogado legalmente inscrito.

Embora a ICP-Brasil tenha sido criada para dar a fé pública às assinaturas eletrônicas, em 2002, a Ordem dos Advogados do Brasil (OAB) criou a sua própria ICP. A ICP-OAB foi criada para emitir os CIs aos seus advogados afiliados. Isto ocorreu, pois existe uma discussão jurídica (ICP-OAB, 2007b) sobre a legalidade do monopólio da ICP-Brasil.

A existência dessas duas ICPs independentes seria um problema potencial, pois, de acordo com a legislação, apenas as assinaturas digitais da ICP-Brasil têm validade jurídica (exceto nos casos em que existe uma aceitação expressa das partes envolvidas).

Os certificados emitidos pela ICP-Brasil têm o objetivo de identificar o usuário. Por outro lado, os certificados ICP-OAB (2007a) têm o claro objetivo de qualificar o usuário como um advogado devidamente inscrito na ordem. São dois certificados com objetivos diferentes.

Para exemplificar a situação, o e-CPF (certificado da ICP-Brasil) identifica o “José da Silva”, mas não o qualifica como advogado. Em contrapartida, o certificado da ICP-OAB, qualificaria “José da Silva” como advogado, mas não garante a legalidade de uma assinatura digital realizada com o certificado, pois o seu certificado não foi emitido por uma AC sob a árvore de certificação da ICP-Brasil.

Este cenário ocorreu até 2008, quando a OAB resolveu firmar uma parceria com a empresa Certisign para emitir os certificados digitais de identidade aos advogados emitidos por uma AC no âmbito da ICP-Brasil, AC-OAB. Esta parceria acabou de vez com a discussão sobre a legalidade do monopólio da ICP-Brasil e embora ainda ativa, a ICP-OAB deve cair em desuso, por falta de legislação que a suporte.

Ainda assim, o novo certificado digital que está sendo emitido possui as mesmas características do e-CPF, ou seja, além de efetuar a identificação, faz-se também a qualificação do titular (neste caso, o de “advogado”).

6.2 Restrições de uso

Os certificados emitidos pela AC-OAB ainda têm problemas com relação à definição exata da limitação de uso do certificado. Ora indica que o uso se limita às atividades profissionais do advogado, ora indica que o uso é igual ao de um certificado digital de identidade comum do âmbito da ICP-Brasil. A seção 1.3.5.1 da Política de Certificado (PC) de Assinatura Digital Tipo A3 da AC-OAB limita o uso do certificado com a apresentação do seguinte texto: “Os certificados emitidos pela AC-OAB no âmbito desta PC, incluindo o hardware criptográfico fornecido, são utilizados exclusivamente para atividades profissionais, no regular exercício profissional do titular. É vedada a utilização dos certificados emitidos pela AC-OAB, bem como os hardwares criptográficos correspondentes para quaisquer outras atividades...”. E a seção 1.3.5.6 da mesma PC refere-se ao documento “Termo de Titularidade” como o indicador das restrições de uso. O referido documento indica o uso geral para certificado, conforme descrito na sua seção 5 sobre o uso e validade do certificado: “Os certificados emitidos pela AC OAB podem ser utilizados em aplicações para a confirmação da identidade do TITULAR e assinatura de documentos eletrônicos e verificação da integridade de informações...”.

6.3 Proposta

Nesta análise, será realizado um ensaio de uso da tecnologia dos CAs que poderá ser adotado por uma entidade de classe como a OAB. Neste ensaio será mantida a

prerrogativa exclusiva da entidade no credenciamento dos advogados e, ao mesmo tempo, será atendida a legislação vigente (BRASIL, 2001), que define a legalidade das assinaturas digitais feitas pelos CI emitidos sob a ICP-Brasil.

Por meio deste trabalho, espera-se mostrar que usar um CA vinculado a um CI é uma alternativa viável para a devida identificação e qualificação de uma pessoa. Dessa forma, sistemas que exijam segurança nas transações eletrônicas podem fazer uso dessa tecnologia para autenticar e conceder permissões para os usuários realizarem tarefas exclusivas às suas atribuições profissionais, com toda a segurança que a tecnologia de criptografia que os certificados digitais de identidade oferecem (REZENDE, 2000).

O uso do CA permite que profissionais ligados às entidades de classe como a OAB, realizem tarefas exclusivas às suas atribuições. Nesta proposta é abordada a entidade OAB. Entretanto a tecnologia dos CA pode ser aplicada a qualquer entidade de classe profissional.

Espera-se também, mostrar que o uso de um certificado digital exclusivamente para a qualificação de um profissional e outro totalmente distinto, mas vinculados logicamente, somente para a identificação da pessoa, facilita e contribui para a administração (emissão, revogação e manutenção do banco de dados) dos certificados digitais (PERMIS, 2007).

Os CAs têm sido usados com sucesso na Espanha para designar o atributo “advogado”, conforme apresentado na seção 2.2.2. Isto reforça a viabilidade da proposta.

6.3.1 Infraestrutura

Nesta seção serão analisados todos os componentes da infraestrutura necessária para o uso e funcionamento da tecnologia de CA pela OAB.

6.3.2 Componentes

A Tabela 3 apresenta os componentes da IGP da OAB.

Tabela 3 - Componentes da IGP da OAB.

Fonte de Autoridade	OAB
Autoridade de Atributo (AA)	Seccionais estaduais da OAB
Usuário do CA ou declarador de privilégio	Advogado
Verificador de privilégio	Qualquer sistema que necessite verificar a condição de advogado devidamente inscrito na OAB.
Lista de Certificados de Atributos Revogados	Esta lista deve ser mantida pela OAB para ser consultada pelos sistemas verificadores de privilégios.

Fonte: elaborado pelo autor (2010)

Nesta IGP, a FAA é a OAB, pois é dela a prerrogativa legal de definir quem é ou não é um advogado. As AAs são as seccionais estaduais da OAB, pois são elas que emitem os CAs diretamente ao advogado.

O usuário do CA ou o declarador de privilégios é o próprio advogado, no momento em que este for usar algum sistema eletrônico que exija as credenciais de advogados para permitir liberar acessos ou realizar tarefas específicas. Estes sistemas eletrônicos devem sempre fazer o papel de verificadores de privilégios quando permitirem ou negarem um acesso.

E, finalmente, a LCAR deve ser mantida pelas seccionais da OAB (AA), para permitir que um sistema usuário possa verificar o estado de revogação dos CAs de advogados, pois atualmente o registro na OAB deve ser renovado anualmente, por meio de pagamento de uma taxa.

6.3.3 Vínculo ao CI

Como visto na seção 3.5, o vínculo do CA ao CI pode ser realizado de várias formas. A sugestão é o uso do RIC. Esta forma de vínculo é mais adequada, pois não existe a obrigatoriedade de se vincular um determinado CI ao CA de advogado. Qualquer CI aceito legalmente (sob normas da ICP-Brasil) e válido pode ser usado para fazer a identificação da pessoa, desde que possua em seu corpo o número do RIC.

Ainda existem dúvidas sobre a restrição de uso dos CI emitidos pela AC-OAB (seção 6.2). Caso se confirme que o certificado deve ser utilizado apenas para atividades profissionais do advogado, ainda não existe a possibilidade de se efetuar o mesmo mapeamento com CI de uso geral e o CA de advogado.

6.3.4 Funcionamento

Nesta seção serão abordados os mecanismos de emissão e uso dos CA, o funcionamento do verificador de privilégios e por fim o funcionamento dos mecanismos de revogação do CA de advogados.

6.3.4.1 Emissão

Um advogado solicita à uma das seccionais estaduais da OAB a emissão do seu CA de advogado.

Para isto, apresenta como credencial de identificação o seu RIC. Note que não existe a obrigatoriedade de apresentar um CI neste momento, pois ele não é usado para emitir o CA. A única informação necessária para emitir o CA é o RIC, não sendo necessária inclusive, a presença física do advogado. Esta característica do CA é interessante, pois torna o funcionamento simples e sem burocracia.

A AA verifica se a pessoa com aquele RIC é de um advogado devidamente inscrito na ordem e verifica, também, se as obrigações das taxas anuais pagas pelo advogado para a entidade estão em dia. Caso esteja tudo em ordem, o CA de advogado é emitido e assinado digitalmente usando o CI da AA.

Neste CA, está informado apenas que determinado RIC pertence a um advogado.

6.3.4.2 Uso

Quando um advogado precisa fazer uso do seu CA, a primeira atividade que deve ser realizada é a sua devida identificação. Este processo deve ser realizado pelos sistemas por meio da apresentação do seu CI e do uso da sua chave privada.

Logo após a identificação, o advogado deve apresentar o seu CA. Só então o sistema liberará os acessos exclusivos aos advogados.

Por meio deste CA, o advogado passa a ser identificado como tal e pode praticar atos como assinar documentos eletrônicos processuais que somente advogados poderiam assinar, acessar áreas restritas de sites do poder judiciário e, também, assinar documentos em nome de terceiros, embora esta última dependa de mecanismos de delegações de privilégios.

Em 2010, existem poucos tribunais que usam CI para os seus mecanismos de autenticação. São eles: o Supremo Tribunal Federal, o Superior Tribunal de Justiça, o Tribunal Superior do Trabalho, os Tribunais Regionais do Trabalho e os Tribunais de Justiça de São Paulo e do Rio Grande do Sul (AASP, 2010).

Nestes sistemas, usa-se apenas o CI para efetuar a autenticação segura. A segurança que apenas um advogado legalmente inscrito realizará acesso ao sistema é feito apenas por meio de um cadastrado prévio do usuário. A verificação desta credencial é manual e, portanto sujeita a falhas. Caso a apresentação desta credencial fosse realizada com CA, a segurança de todo o processo seria muito maior, delegando inclusive a responsabilidade da entrega do atributo “advogado” ao usuário à OAB.

6.3.4.3 Verificador de privilégios

Quando o usuário apresenta o seu CA, o verificador de privilégios deve verificar o seguinte:

- se o CA está dentro do prazo de validade;
- se o CA foi assinado por AA credenciada da OAB;

- se o CI da AA é válido;
- se o atributo descrito no CA é o necessário para a liberação dos recursos protegidos;
- se o CA não foi revogado.

6.3.4.4 Revogação

Caso o período de validade definido para o CA de advogado seja mantido em 1 ano como é atualmente, as AAs devem manter a LCAR. Caso o período seja mais curto como, por exemplo, algumas horas (FARRELL et al, 2010), não seria necessária a manutenção desta lista e conseqüentemente os sistemas verificadores não necessitariam fazer este tipo de verificação.

A definição do período de validade do CA de advogado vai depender da disponibilidade e da capacidade da AA emitir CAs online (para o caso de validade de algumas horas), além do mecanismo de emissão do CA: se por meio "*push*", no qual o CA é entregue ao portador ou se pelo meio "*pull*" no qual o CA é gerado a cada consulta ao sistema (FARRELL et al, 2010).

O número de advogados que anualmente são expulsos da OAB é pequeno, se comparado com o número de profissionais cadastrados. Entretanto, é importante não permitir que um profissional expulso da entidade continue a atuar clandestinamente. Como exemplo, a OAB-SP expulsou 17 advogados em 2005 (OAB, 2006).

Com base nestes números, este estudo de caso propõe a adoção do modelo "*push*" de emissão, com o período de um ano de validade e a manutenção de uma LCAR.

A LCAR poderia, também, ser usada para suspender temporariamente o advogado, muito utilizado nos casos em que a OAB está avaliando um processo de expulsão ou quando pretende impor punições a seus associados.

6.4 Análise da proposta

Esta seção efetua a análise crítica da proposta de uso de CA para o atributo “advogado”.

6.4.1 Segurança

Esta seção analisa a viabilidade do uso de CAs relacionada à segurança.

Os sistemas dos tribunais podem usar basicamente as seguintes formas para efetuar a autenticação de advogados:

a) com certificado digital de identidade de uso geral;

b) com certificado digital de identidade com o atributo “advogado”;

c) sem certificado digital.

6.4.1.1 Com certificado digital de identidade de uso geral

Comparativamente à proposta de uso de CA de advogado com a utilização do certificado digital de identidade de uso geral (atualmente adotado pelos tribunais), a segurança do processo de autenticação é exatamente a mesma, uma vez que é usado o CI para isto.

Para o processo de concessão de privilégios, com uso de CA, a definição do atributo “advogado” concedida pela OAB à pessoa, torna o sistema de concessão de privilégios mais segura, uma vez que a concessão do atributo ocorre que forma descentralizada. Nos sistemas atuais a definição do atributo “advogado” é realizada por um cadastro prévio nos sistemas dos tribunais. A verificação da autenticidade da informação deve ser feita manualmente e, portanto, passível de falhas.

6.4.1.2 Com certificado digital de identidade com o atributo “advogado”

Nos certificados emitidos pela AASP, por exemplo, o atributo “advogado” está inserido no corpo do certificado. Este fato melhora a segurança e comparado com a proposta não existe diferenças na segurança tanto da autenticação como na

concessão dos privilégios. Entretanto, ainda não existe na prática, a obrigatoriedade do CI usado para se autenticar nos sistemas contenha o atributo “advogado” no seu corpo. Os tribunais ainda não estão preparados para efetuar a leitura do atributo advogado que podem estar contidos no corpo do CI e também não conseguiriam verificar o prazo de validade do atributo, uma vez que ele não está presente no certificado.

6.4.1.3 Sem certificado digital de identidade

Ainda que não exista um sistema que use a autenticação efetuada por um certificado digital de identidade, é possível que o CA de advogado seja usado exclusivamente para a concessão de privilégios.

Comparativamente à proposta de uso de CA de advogado com os sistemas que não adotam os certificados digitais, a segurança do processo de autenticação é exatamente a mesma, ou seja, não disponibiliza a força da segurança da autenticação efetuada com certificado digital.

Com relação ao processo de concessão de privilégios, com uso de CA, a definição do atributo “advogado” emitida pela OAB ao titular, promove uma segurança maior na concessão de privilégios. Entretanto, a segurança mais adequada só é obtida com o uso concomitante do CI e do CA de advogado.

6.4.2 Gestão dos atributos e certificados

No sistema atual a gestão do atributo “advogado” é realizada pela OAB que contrata uma empresa privada para operar a AC. Nesta situação, existe a necessidade de um canal seguro entre a OAB e a AC emissora do CI para que o atributo “advogado” seja informado.

Na proposta, a prerrogativa de administrar o atributo “advogado” continua sendo normalmente efetuada pela OAB. A diferença reside no fato de que não é necessário que a OAB tenha uma conexão segura com a AC emissora do CI para informar o atributo “advogado”, uma vez que esta informação não é armazenada no CI.

No sistema atual, como o atributo “advogado” encontra-se junto com o CI, existe o problema da revogação. Caso o atributo seja revogado, o CI também deve ser cancelado. Outro problema refere-se ao prazo de validade. O CI do tipo A3 possui três anos de validade e o atributo “advogado” deve ser validado anualmente por meio do pagamento das taxas da categoria de classe. Esta incompatibilidade de prazos afeta a validade do CI.

Na proposta, como há independência de certificado, os problemas mencionados anteriormente relativos à revogação e o prazo de validade são minimizados. Os certificados possuem o seu próprio mecanismo de revogação e prazo de validade. Desta forma a revogação do CA de advogado não afeta o CI e vice-versa, assim como os prazos de validade não interferirem na vida útil do outro certificado. O CI do tipo A3 pode continuar a ser usado por 3 anos e o CA de advogado pode ser emitido anualmente.

Como este estudo de caso propõe a adoção do modelo “*push*” de emissão, com o período de um ano de validade, existe a necessidade de se manter uma LCAR.

6.4.3 Legalidade

A legalidade do uso de CA para o atributo “advogado” é garantida pela mesma lei que criou os certificados digitais de identidade (BRASIL, 2001). Por meio desta lei, as assinaturas eletrônicas efetuadas com certificados digitais de identidade da ICP-Brasil têm validade jurídica e, portanto, devem ser aceitos universalmente pelos sistemas usuários. O CA é um documento assinado digitalmente por um certificado emitido por uma AC subordinada à AC raiz da ICP-Brasil e por isso deve ser legalmente aceito.

No estudo apresentado, a prerrogativa legal da OAB de designar o atributo “advogado” foi mantida. Isto significa dizer que não há alteração legal neste sentido.

6.4.4 Interoperabilidade

Uma das vantagens do uso de CA é a padronização do formato do certificado e do próprio atributo. Com a padronização, permite-se que sistemas heterogêneos possam usar estes certificados nos seus mecanismos de autorização.

No momento em que AA-OAB emite o CA de advogado, não é relevante a informação de quais sistemas farão uso deste certificado. Desta forma a utilização não se limita apenas aos sistemas de determinados domínios (somente no judiciário, por exemplo). Qualquer sistema que necessite da credencial “advogado” pode fazer uso deste CA na liberação de acesso aos seus recursos.

Com relação à interoperabilidade do CI, ressalta-se que a substituição de um CI com o atributo “advogado” por um CI de uso genérico pode beneficiar as aplicações haja vista a atual restrição de uso imposta para os CIs com o atributo “advogado”.

6.5 Exemplos de aplicabilidade

A aplicabilidade deste tipo de CA se estenderia para qualquer entidade de classe. O mesmo formato de CA apresentado neste estudo de caso poderia ser utilizado nos seguintes atributos e suas respectivas fontes de autoridade:

- Médico - CFM;
- Enfermeiro - CFE;
- Administrador - CFA;
- Contador – CFC; etc.

6.6 Conclusão

Este estudo de caso apresentou o uso de CA para efetuar a ligação entre uma pessoa física e uma entidade de classe.

O uso de CA para este propósito pode ser muito útil para estas entidades. A criação de IGPs ao invés de ICPs facilita a administração dos certificados, uma vez que são certificados que dispensam o uso de senhas, mantendo as prerrogativas legais das

entidades como fontes de autoridade de atributos, oferecendo os mesmos níveis de segurança existente nos mecanismos de autenticação efetuados com CI e com a cobertura legal da legislação vigente.

O estudo de caso apresentou o caso da OAB. Entretanto, outras entidades de classe (como, por exemplo, o Conselho Federal de Contabilidade) têm optado por emitir CIs ao invés de CAs. Como a complexidade da montagem, operação e manutenção de um AC é alta, as entidades de classe têm se associado a ACs de empresas privadas. Estas associações, embora legais e operadas satisfatoriamente, são desnecessárias. Bastaria um CI para efetuar a autenticação e vários CAs poderiam ser usados para efetuar a autorização de acessos. Isto mostra o total desconhecimento das entidades neste tipo de tecnologia.

Especificamente sobre este estudo de caso, os sistemas dos tribunais têm usado os CIs apenas para efetuar a autenticação dos usuários. Ainda faltam alguns serviços que devem usar os certificados digitais para melhorar estes sistemas:

a) assinatura digital em petições;
b) múltiplas assinaturas em documentos;
c) controle temporal (carimbo de tempo), uma vez que a contagem de prazo é um item importante para o judiciário;
d) intimações, protocolos, procurações, substabelecimento, entre outros.

7 ESTUDO DE CASO: CADASTRO DE PESSOA FÍSICA (CPF)

Nesta seção será apresentado o estudo de caso do cadastro da pessoa física (CPF) na Receita Federal do Brasil (RFB) e viabilidade de utilização de CA neste contexto.

O CPF foi selecionado para ser objeto de estudo porque é uma situação na qual podem ser analisadas aplicações usando o CPF convencional (não digital) e também aplicações que usam o e-CPF. O e-CPF é um certificado digital de identidade com o atributo CPF, emitido por uma AC subordinada à AC da Receita Federal no âmbito da ICP-Brasil.

Para o CPF em formato convencional será analisada a aplicação existente atualmente no site da RFB disponível ao público que verifica o nome e a situação cadastral de uma pessoa física.

A aplicação analisada com o uso do e-CPF é o atendimento eletrônico da PF na RFB.

Para cada uma das situações analisadas, é apresentada uma proposta de funcionamento da mesma aplicação com o uso do CA e uma análise comparativa do sistema atual e o proposto.

7.1 1ª Aplicação: consulta nome e situação cadastral de CPF por um sistema qualquer fora do domínio da RFB

Nesta seção é apresentado o estudo de caso sobre aplicação existente atualmente na RFB para a consulta de nome e situação cadastral do CPF.

7.1.1 Sistema atual

Atualmente, a consulta de situação cadastral de CPF é realizada pelos usuários para checar o nome de uma pessoa e a sua situação cadastral. Esta consulta só pode ser realizada nas situações em que se conhece o CPF da pessoa consultada. A consulta inversa, ou seja, quando o usuário conhece o nome e deseja descobrir o CPF só é possível de ser realizada nos postos de atendimento da RFB (RFB, 2009a).

A Figura 7 mostra um exemplo de tela de consulta obtida no site da RFB.

Ministério da Fazenda
Secretaria da Receita Federal do Brasil

Comprovante de Inscrição e de Situação Cadastral no CPF

Nº do CPF: 131.343.[redacted]-[redacted]

Nome da Pessoa Física: CELSO FUKUSHIMA

Situação Cadastral: REGULAR

Comprovante emitido às: **20:56:51** do dia **08/09/2009** (hora e data de Brasília).

Código de controle do comprovante: **2DE5.665F.88B2.CD49**

A autenticidade deste comprovante deverá ser confirmada na página da Secretaria da Receita Federal do Brasil na Internet, no endereço www.receita.fazenda.gov.br.

Aprovado pela IN/RFB nº 864, de 25/07/2008.

Figura 7 - Tela de consulta do CPF

Fonte: site da RFB (2009)

Como ainda não existem meios eletrônicos seguros implementados, o site da RFB gera um código de controle de comprovante que pode ser usado para a verificação de autenticidade da consulta. O resultado desta verificação é mostrado na Figura 8.

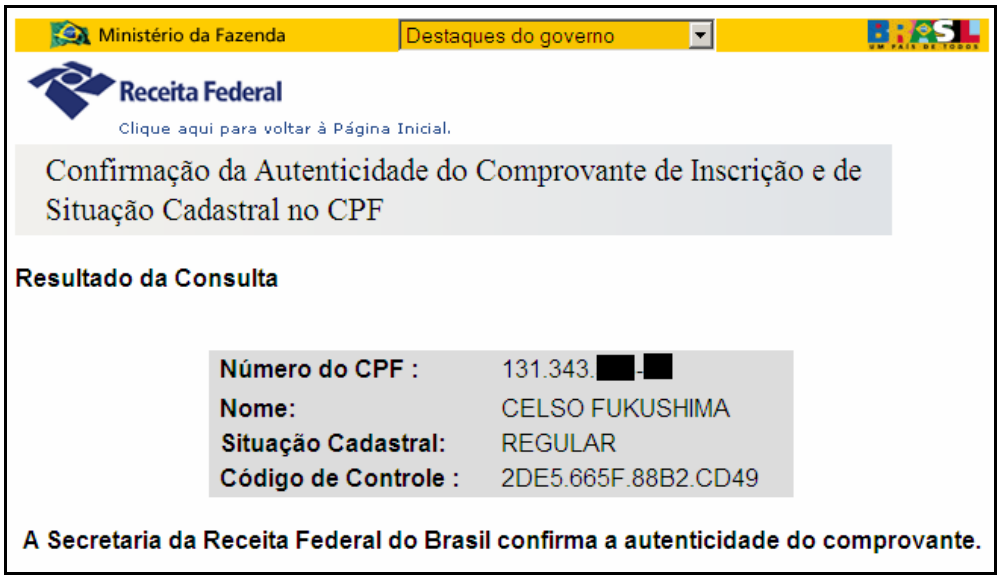

Figura 8 - Tela de confirmação de autenticidade da consulta do CPF da RFB

Fonte: site da RFB (2009)

Observa-se que todo o processo atual apesar de eletrônico, depende de intervenção humana para realizar acesso ao site e realizar a consulta e não existem sistemas automatizados para efetuar este tipo de consulta, o que inviabiliza o seu uso para efetuar validações de CPF em uma transação eletrônica.

Além disso, para evitar que ocorram fraudes sobre este tipo de consulta, a RFB criou um mecanismo de verificação de autenticidade da consulta. Este procedimento é útil para a prevenção de fraudes, entretanto dependem sempre de uma consulta on-line ao site da RFB, além do elemento humano para a verificação visual da informação.

7.1.2 Proposta

Para este cenário é proposto um sistema na RFB que emita um CA no qual constam os atributos “CPF”, “nome” e “situação cadastral” de uma pessoa física (PF) a partir de uma solicitação de qualquer sistema usuário que apresente um RIC para ser verificado.

7.1.3 Tipo de Emissão do CA

Para emissão de CA pode ser usado tanto o tipo “*pull*” quanto o tipo “*push*”, dependendo dos requisitos de segurança do sistema usuário.

No modelo “*push*”, com um CA com validade de 1 ano, cabe ao titular do CA apresentá-lo quando solicitado. Quando o CA é emitido, o titular deve armazená-lo para que possa ser apresentado quando requisitado por uma aplicação. A aplicação, ao receber um CA, deve realizar a validação de CA. Neste caso, dentre as diversas validações necessárias, é necessário verificar o estado de revogação. Para isso, é necessário realizar um acesso *online* ao repositório da RFB para a obtenção da LCAR e anexá-la, também, ao processo a fim de possibilitar uma validação futura.

Outra alternativa seria a utilização do modelo “*pull*”. Neste tipo, um CA será gerado a cada consulta que a aplicação usuária realiza no site da RFB.

Nesta proposta, a sugestão para as aplicações é a adoção do modelo “*pull*”. Toda vez que for efetuada uma transação, um CA será emitido pelo site da RFB que será anexado à transação.

7.1.4 Prazo de validade e LCAR

Para o tipo “*push*” de emissão, o prazo de validade é longo (mais do que algumas horas é considerado longo por FARRELL et al (2010)), então é necessária a criação e manutenção de uma LCAR.

Por outro lado, caso o tipo “*pull*” seja adotado, usam-se períodos curtos de validade, da ordem de alguns dias, dispensando a manutenção de uma LCAR.

A decisão de manter ou não uma LCAR é importante, pois implica em ter ou não o custo operacional de verificação de revogação e cancelamento dos CAs.

Nesta proposta, a sugestão é definir curtos períodos de validade do CA, de tal forma que seja emitido um CA para cada transação e assim não seja necessária a manutenção de uma LCAR.

7.1.5 Classe de Aplicabilidade e Vínculo ao portador

As Classes de Aplicabilidade (tratadas na seção 3.4) deste CA envolvidas nesta aplicação são as seguintes: “vínculo a uma entidade”, neste caso a indicação que a pessoa (com o determinado nome e CPF) está inscrita no cadastro da RFB, sendo portanto um “contribuinte da RFB”; e a “atribuição de estado”, com a indicação da sua situação cadastral.

O campo RIC é sugerido para fazer o vínculo do CA ao portador (Figura 9), conforme apresentado na seção 4.3.

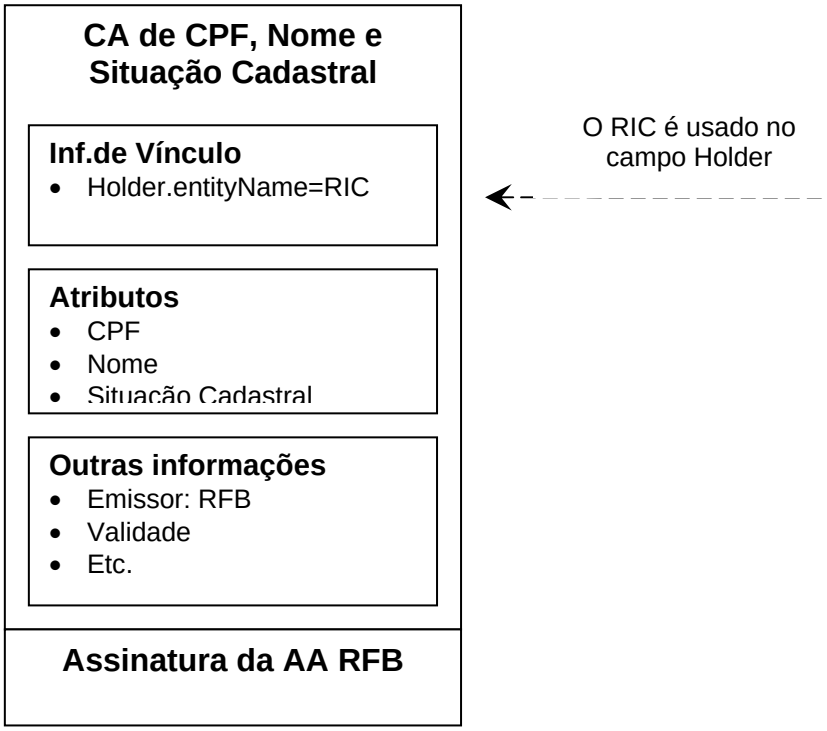

Figura 9 - O RIC como vínculo à entidade em um CA de verificação de CPF, Nome e Situação Cadastral

Fonte: elaborado pelo autor (2010)

7.1.6 Análise da proposta

Nesta seção é realizada a análise comparativa da aplicação atual em relação à proposta.

7.1.6.1 Segurança

No sistema atual, com relação à segurança da transação, a garantia de autenticidade do primeiro documento, o “Comprovante de Inscrição e de Situação Cadastral no CPF”, é realizada pela emissão de um segundo documento, a “Confirmação de Autenticidade da Consulta do CPF”. Neste mecanismo, a verificação de autenticidade é manual e visual, além de depender de uma conexão ao site da RFB.

Uma vez efetuada esta consulta, o resultado deve ser impresso e anexado à documentação da transação que se deseja validar. Uma validação no futuro depende também de um acesso ao site da RFB.

Neste processo há uma lacuna de segurança, pois uma pessoa mal-intencionada poderia criar falsas consultas e fraudar a validação desta consulta. Uma vez feito isto, estes documentos forjados poderiam ser impressos e anexados à transação como parte da sua documentação. Esta fraude poderia ser identificada apenas com a verificação manual e visual da validação da consulta no site da RFB, mas não poderia ser feita de forma automatizada.

Na proposta, a garantia de validade do CA é dada pela assinatura digital realizada pela RFB presente no certificado.

Além de melhorar a segurança e automatizar o processo de validação, esta proposta abre a possibilidade de efetuar verificações completas de transações em formato eletrônico.

Esta característica é bastante desejável em função das inúmeras aplicações usuárias que precisam deste recurso. Nos mais variados tipo de contrato existente no mundo real é encontrada a necessidade de efetuar validações de CPF, nome e situação cadastral na RFB.

Atualmente, a necessidade de verificar a validade de um CPF e correspondente nome do contribuinte já é uma demanda de vários sistemas, motivo pelo qual a RFB disponibilizou o atual serviço manual.

7.1.6.2 Gestão dos atributos e certificados

No sistema atual não existem certificados envolvidos. Todo o processo ocorre de forma eletrônica, mas por meio de páginas da internet. Na proposta, os resultados das consultas são transformados em CA. Comparativamente, no sistema atual é necessário que a RFB mantenha mecanismos que verifiquem a autenticidade das consultas, ou seja, a RFB deverá manter para sempre este sistema, caso queira permitir a validação de consultas efetuadas em qualquer data. Na proposta, não existe esta necessidade, pois o CA será assinado digitalmente pela RFB. Esta assinatura por si só, garante a sua autenticidade. As verificações futuras de autenticidade do CA podem ser realizadas por meio desta assinatura sem a necessidade de conexão com o site da RFB. Desta forma, houve um ganho significativo no processo, pois a RFB não necessitaria de manter mecanismo de verificação de autenticidade da consulta

7.1.6.3 Legalidade

O embasamento legal da proposta é dado pela legislação vigente que reconhece a legitimidade das assinaturas digitais realizadas com os CIs da ICP-Brasil. O CA de CPF é um documento assinado digitalmente por um certificado emitido por uma AC no âmbito da ICP-Brasil e por isso deve ser legalmente aceito.

Outro aspecto relativo à legalidade do processo refere-se manutenção da prerrogativa da RFB de designar o atributo “contribuinte”. Isto significa dizer que não há alteração legal neste sentido.

7.1.6.4 Interoperabilidade

Para este cenário a interoperabilidade é obtida pela padronização no formato do certificado. Nesta aplicação, existe a presença de alguns atributos e a padronização deles é relevante para que os sistemas de qualquer domínio possam efetuar consultas, extrair os dados e armazenar o CA para possibilitar a verificação futura.

A interoperabilidade permite, por exemplo, que um mesmo CA (obtido em uma consulta) possa ser utilizado por vários sistemas. Esta característica é bastante

desejável, uma vez que com o aumento do reuso do certificado, reduz-se a quantidade de consultas no site da RFB.

7.1.7 Conclusão

Neste estudo de caso foi apresentada uma proposta de utilização de CA para a verificação de CPF, nome e situação de cadastral de contribuintes, com a apresentação do RIC. Esta proposta mostra-se viável do ponto de vista tecnológico, segura e legal.

Esta aplicação pode substituir o atual sistema manual de verificação disponível na Internet no site da RFB com vantagens:

- efetuar validações automatizadas;
- permitir efetuar validações de toda uma transação em formato eletrônico;
- coibir fraudes;
- e garantir a segurança de todo o processo.

7.2 2ª Aplicação: atendimento eletrônico de Pessoa Física

O atendimento eletrônico da pessoa física da RFB foi selecionado para ser objeto de estudo porque é uma aplicação no qual é utilizado um certificado digital de identidade do âmbito da ICP-Brasil, o e-CPF, que contém o atributo CPF do titular.

Este estudo de caso considera as situações nas quais o cidadão possui um CI e deve ser cadastrado na RFB, ou seja, possuir um CPF. O motivo desta restrição é que atualmente é possível emitir um CI sem que a pessoa possua um CPF. Esta situação é permitida para estrangeiros (ITI, 2009), porém este tipo de CI não pode ser usado para acessar os serviços da RFB e, portanto, fora do escopo deste estudo de caso.

Inicialmente será apresentado o perfil atual do e-CPF e o seu funcionamento no atendimento eletrônico disponível pela RFB. Em seguida será apresentada uma proposta para a mesma aplicação, mas desta vez com o uso do CA para o atributo

CPF. Posteriormente será realizada uma análise comparativa entre os dois sistemas e finalmente será apresentada a conclusão deste estudo de caso.

7.2.1 Sistema atual

A análise do CI e-CPF mostra sua aderência ao perfil centralizado (PERMIS, 2007) ou estrutura monolítica (PARK, 2000), conforme apresentado na seção 3.6.1, pois nele estão contidas informações de identificação e de qualificação do titular.

As informações de identificação são aquelas inerentes ao portador e, no CI ICP-Brasil de PF são os seguintes campos:

a) nome: obrigatório e deve ser incluído no campo *Subject* no formato *Distinguished Name (DN)* do padrão ITU X.500/ISO 9594*,* no subcampo *Common Name (CN)*. Este campo não pode ter mais do que 54 caracteres e não podem existir abreviações;

b) data de nascimento: obrigatória e deve ser incluída no campo de extensão *SubjectAlternativeName* nas 8 primeiras posições do OID 2.16.76.1.3.1 no formato ddmmaaaa.

Além das informações de identificação também estão presentes outras que qualificam o titular como, por exemplo, no e-CPF, o CPF e Título de Eleitor:

a) CPF: obrigatório (no e-CPF) e deve ser incluído no campo *SubjectAlternativeName* a partir da 9º posição do OID 2.16.76.1.3.1 (ITI, 2006), ocupando 11 dígitos, ou seja, sem traços e pontos. O CPF indica que a pessoa está inscrita na RFB e a qualifica como “contribuinte da RFB”;

b) no. do título de eleitor: obrigatório e deve ser incluído no campo *SubjectAlternativeName* sob OID 2.16.76.1.3.5 (ITI, 2006). O título de eleitor indica que a pessoa está inscrita no cartório eleitoral e a qualifica como eleitor.

A característica de manter dados de identificação junto a dados de qualificação é uma desvantagem existente no e-CPF.

Conforme apresentado em PERMIS (2007), a outra alternativa, a adoção de um perfil descentralizado no qual existe a separação nos certificados das funções de identificação (ICP) e de qualificação (Infraestrutura de Gerenciamento de Privilégio – IGP) apresenta vantagens em relação ao perfil centralizado, como a facilidade de administração na emissão e revogação dos certificados e na manutenção dos bancos de dados.

Uma vantagem existente no e-CPF é a facilidade de verificar o vínculo entre o atributo CPF e o CI, uma vez que eles estão no mesmo certificado (PARK, 2000). Esta característica facilita a validação das credenciais pelos mecanismos de autenticação e liberação de acessos dos sistemas usuários.

A outra característica existente no e-CPF é a presença de um identificador único (o número do CPF) para todos os contribuintes da RFB. Esta característica é bastante desejável, pois facilita a identificação das pessoas. Entretanto, o CPF não pode ser usado com um identificador único conforme mostra a Figura 10.

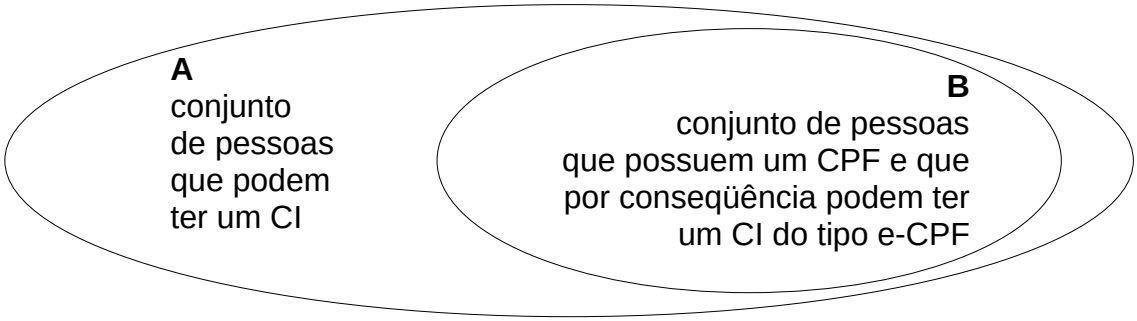

Figura 10 - Conjunto de pessoas que podem ter um CI contém o conjunto de pessoas que possuem um CPF

Fonte: elaborado pelo autor (2010)

Na Figura 10, o conjunto **A**, formado pelas pessoas que podem ter um CI é diferente do conjunto **B** formado pelas pessoas que possuem o CPF. Ou seja, o CPF pode não estar presente em um CI e, portanto, não pode ser usado como identificador único.

Isto seria possível apenas se todos os CIs tivessem obrigatoriamente um CPF (**A** estivesse contido em **B** ou se **A** fosse igual a **B)**. Para o campo ser usado como um identificador único, ele deve estar presente em todo o conjunto **A** e não é o que ocorre: estrangeiros podem ter um CI e não são obrigados a ter um CPF (ITI, 2009).

O e-CPF é um documento eletrônico (RFB, 2008c) emitido por uma AC credenciada pela AC-Raiz da ICP-Brasil e habilitada pela AC-RFB. Não podem ser titulares de certificados e-CPF as pessoas físicas cuja situação cadastral perante o CPF esteja enquadrada na condição de cancelado. Esta condição é necessária pois, durante o processo de emissão do e-CPF, ocorre a verificação da validade do CPF (RFB, 2008c).

A fonte de autoridade para a emissão do CPF é a RFB e a fonte de autoridade para a emissão de um CI são as ACs credenciadas pela ICP-Brasil. Isto posto, verifica-se que na emissão do CI e-CPF, e como tal teria apenas uma fonte de autoridade (AC emitente), foi incorporado mais uma entidade, a RFB que é a validadora do CPF, ou a fonte de autoridade do atributo CPF.

Neste formato de CI, existe um problema com relação ao período de validade do e-CPF: atualmente o CPF deve ser validado todo ano sob pena do contribuinte ter o seu CPF suspenso. A revalidação pode ser feita por meio da declaração anual de imposto de renda, da declaração anual de isentos ou por meio de formulário apropriado disponíveis nos agentes autorizados (RFB, 2009b).

O e-CPF tem uma validade que varia de 1 ano (A1) a 3 anos (A3), dependendo do tipo e da mídia de suporte. Com estas duas situações, verifica-se que independentemente da validade do e-CPF, o titular deve anualmente revalidar o seu CPF; o que gera a seguinte situação incoerente: um e-CPF com validade de 3 anos pode ser revogado antes do término da validade caso o CPF seja suspenso ou cancelado. A validade do CPF só é mantida por meio das revalidações anuais obrigatórias, descritas anteriormente.

Nesta situação, o e-CPF é revogado caso o CPF seja suspenso ou cancelado, antes da validade do e-CPF (Figura 11).

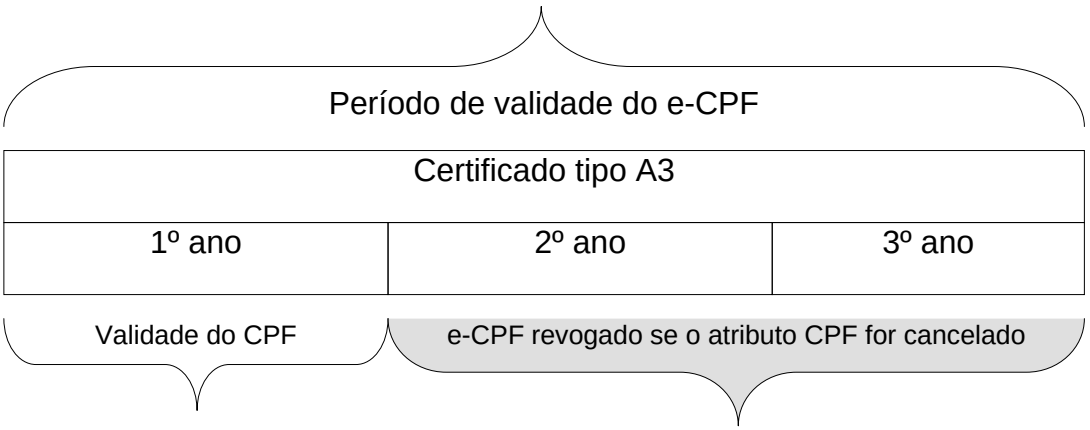

Figura 11 - Incoerência de prazos de validade do atributo CPF no e-CPF

Fonte: elaborado pelo autor (2010)

7.2.2 Proposta

Para este cenário é proposto o uso da tecnologia de CA para o atributo CPF. Para isto há um desmembramento do e-CPF em dois certificados: um CI e um CA. O CI é emitido por uma AC credenciada da ICP-Brasil, da mesma forma que é realizada atualmente, mas sem a presença do campo CPF, e o atributo CPF é emitido no formato de um CA no qual a AA emissora é a RFB.

7.2.2.1 Emissão do CI

O CI deve ser emitido por qualquer AC subordinada à AC-Raiz, mas como o atributo CPF não existe mais no CI, não há a necessidade que a AC emissora esteja sob a árvore de certificação da AC-RFB como ocorre atualmente com o e-CPF.

Todos os CIs, independentemente da AC emissora, têm o mesmo formato padronizado pelas regras da ICP-Brasil e com a função exclusiva de identificação do titular. Ou seja, atributos que qualificam o titular não são incluídos no certificado.

7.2.2.2 Emissão do CA de CPF

Caso o cidadão não possua cadastro de CPF da RFB, deve se inscrever na RFB para se cadastrar como um contribuinte. Este processo deve seguir o trâmite atual para a obtenção do CPF e exigirá que o cidadão possua um documento de identificação emitido pelos órgãos competentes. O documento de identificação mais comum é o Registro Geral (RG) emitido pela Secretaria de Segurança Pública Estadual.

Legalmente, são aceitos como documentos de identificação a Carteira Nacional de Habilitação instituída pela Lei 9.503/97, passaporte expedido pela autoridade competente, RNE – Registro Nacional de Estrangeiro e carteira de exercício profissional emitida pelos órgãos criados por Lei 6.206/75.

Qualquer um destes documentos pode ser usado como campo vinculante do CA ao CI, porém com o advento do RIC (seção 4.3), ele foi adotado neste estudo de caso.

Existem duas formas possíveis de emissão de CA de CPF: “*push*” e “*pull*”.

Na primeira forma chamada de “*push”* (FARRELL et al, 2010), o CA é um documento eletrônico que possui uma validade longa e, por isso, necessita ser armazenado para usar no futuro

Não existe a necessidade de armazenar o CA em meios seguros, pois não há segredo a ser guardado. A verificação com relação à segurança é feita pelos sistemas usuários para checar se o CA é autêntico e está íntegro. Neste mecanismo é usada a chave pública da AA que assinou o CA.

Para um cidadão interagir com segurança com os serviços eletrônicos oferecidos por um sistema que exija o CPF, ele deve apresentar inicialmente o seu CI para realizar o processo de autenticação.

O sistema de autenticação verifica se o CI é válido e realiza o processo de autenticação do usuário, utilizando também a chave privada. Uma vez autenticado, o sistema deve solicitar o CA de CPF. Após a validação do CA CPF e se tratando de um contribuinte cadastrado na RFB, libera-se o acesso aos recursos do sistema, de acordo com o perfil da credencial “contribuinte da RFB”.

Como os certificados estão fisicamente separados e o campo adotado como vínculo entre o CI e o CA foi o RIC, os prazos de vigência dos certificados estão desvinculados, de forma que o CI pode expirar independentemente do CA de CPF e vice-versa. Caso o CI expire antes do CA de CPF, basta o cidadão solicitar um novo CI à AC. Como o RIC é o mesmo (o RIC é único), o antigo CA de CPF pode ser usado com o novo CI, sem a necessidade de uma re-emissão de um novo CA. O inverso também é verdadeiro, pois um novo CA de CPF também pode ser usado com o antigo CI.

Esta forma de CA é usada em ambientes nos quais o titular apresenta o seu CA à aplicação (Figura 12). Desta forma não é necessária uma nova conexão entre o cliente e o servidor para fazer a validação da credencial, eliminando a carga computacional deste processo no servidor. A contrapartida é a necessidade de busca e armazenamento da LCAR, uma vez que o prazo de validade de um CA deste tipo é geralmente longo, ou seja, mais do que algumas horas (FARRELL et al, 2010).

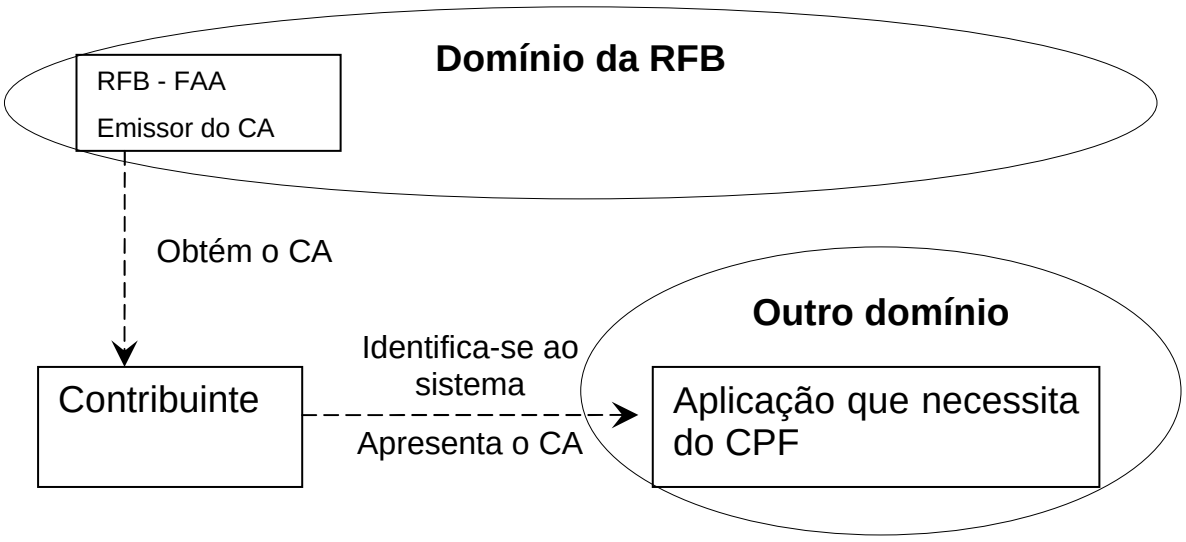

Figura 12 - Emissão "*push*" – o CA é "empurrado" para a aplicação

Fonte: elaborado pelo autor (2010)

A outra forma é chamada de "*pull*"" (FARRELL et al, 2010) (Figura 13) no qual o CA possui validade de menor período e, cabe à aplicação a busca do CA do usuário.

Este tipo de emissão de CA é usado em ambientes nos quais o titular simplesmente se autentica na aplicação e esta aplicação solicita o CA diretamente à AA. O CA que será entregue pode ser gerado a cada solicitação ou estar disponível em algum repositório.

Novamente, neste cenário, a análise mostra mais vantajosa a utilização do modelo "*pull*".

A outra vantagem deste tipo de emissão é que não é necessário manter mecanismos de revogação, pois o prazo de validade do CA será de poucas horas ou dias (FARRELL et al, 2010) o que deixa a infraestrutura mais simples.

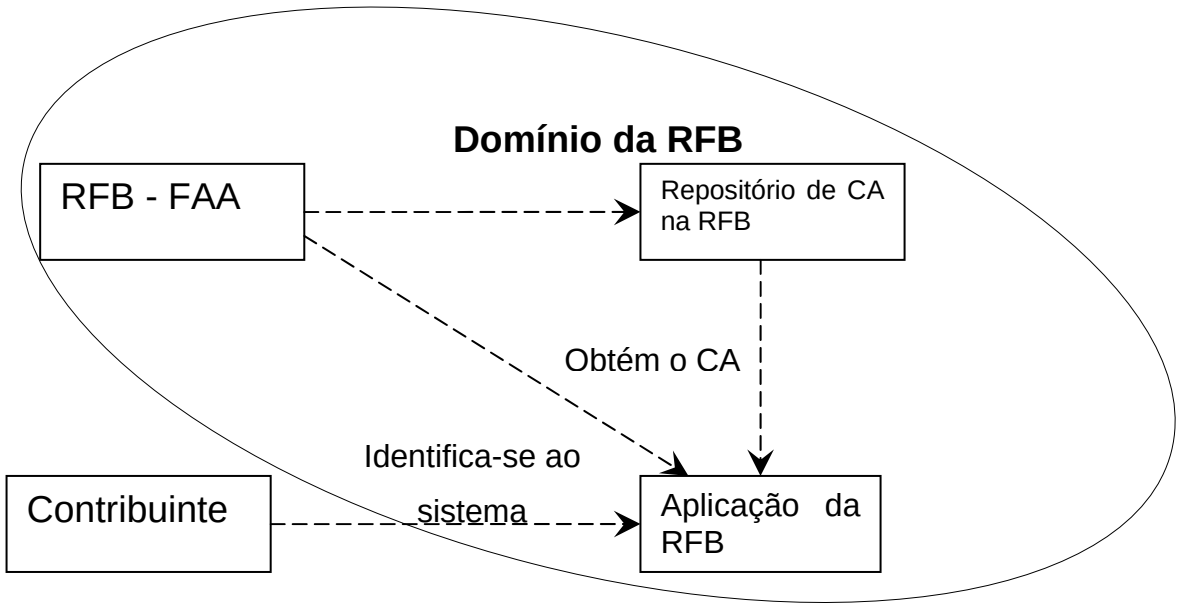

Figura 13 - Esquema de CA CPF com modelo "pull"

Fonte: elaborado pelo autor (2010)

7.2.2.3 Componentes da IGP do CPF

A Tabela 4 apresenta os componentes da IGP de CPF.

Tabela 4 - Componentes da IGP do CPF

Fonte de Autoridade	Receita Federal do Brasil
Autoridade de Atributo (AA)	Receita Federal do Brasil
Usuário do CA	Contribuinte
Verificador de privilégio	Qualquer sistema da RFB
Lista de Certificados de Atributos Revogados	Desnecessária na emissão *"pull"*

Fonte: elaborado pelo autor (2010)

7.2.3 Análise da proposta

Nesta seção será realizada uma análise comparativa do sistema atual com a proposta de uso de um CA CPF.

7.2.3.1 Segurança

Considerando que tanto no sistema atual quanto no proposto, o método de autenticação do usuário é feito usando um CI, não existe diferenciação do ponto de vista da segurança.

Os serviços básicos de segurança (integridade, autenticidade, sigilo e não repúdio) providos pelo CI são completos nas duas situações. Em ambas é possível usar a assinatura digital que garante a integridade, a autenticidade e o não repúdio, dos atos realizados ou declarados pelo usuário. Nas situações que o sigilo é necessário, pode-se usar o recurso da criptografia dos dados usando a chave pública do destinatário.

Supondo que, em alguma aplicação, o processo de identificação não seja realizado por meio de um CI ou que não haja um processo de identificação, o CA apresentado ainda proverá a garantia de que um determinado cidadão portador do RIC é contribuinte cadastrado na RFB sob um determinado CPF. Exemplo: uma aplicação necessita realizar uma transação no qual é preciso que se valide e se declare que

um CPF pertence a uma determinada pessoa. Pode-se solicitar a RFB um CA de CPF, sem que fosse necessário o uso de CI do titular. Este CA poderia ser anexado à documentação daquela transação, comprovando que naquele determinado momento, aquele CPF era válido e pertencia àquela pessoa.

A integridade, autenticidade e o não repúdio do que está presente no CA é garantido pela assinatura digital realizada pelo CI da AA.

7.2.3.2 Gestão dos atributos e certificados

No perfil atual do e-CPF, a AC deve ser uma AC subordinada à AC-Raiz da ICP-Brasil e ao mesmo tempo subordinada à AC-RFB. O processo de emissão deve seguir todos os procedimentos de segurança impostos pelas políticas de certificação definidas pela ICP-Brasil, além da verificação presencial necessária para a emissão de um CI.

Após a emissão do e-CPF, determinadas informações contidas no certificado podem ser alteradas e não mais refletir a realidade. Exemplo: a seção do título de eleitor pode ter mudado ou o CPF pode ter perdido a validade, pois o contribuinte não fez a revalidação anual. Todas as vezes que ocorrer alguma alteração nos dados do e-CPF, ele deve ser revogado.

Na proposta, o CI deve possuir apenas dados de identificação do titular. Dados estes que não são alterados ao longo da vida da pessoa (ou que ao menos possuem baixa freqüência de alteração). Exemplos: data de nascimento, nome e RIC. Esta condição tem o objetivo de aumentar a probabilidade de que o CI esteja operacional ao longo do seu período de validade.

Todas as regras de emissão, manutenção e revogação definidas pela ICP-Brasil para os CIs continuam a serem seguidas normalmente.

Além de reduzir a probabilidade de revogação do CI, o outro diferencial desta proposta é o desmembramento dos períodos de validade do CI e dos atributos, resolvendo o problema apresentado na Figura 11 (pág. 100).

A RFB emite o CA de CPF usando o tipo “*pull*” de emissão, no qual os CAs são gerados por demanda ou são fornecidos por meio de um repositório de certificados,

ou seja, os certificados não são entregues ao titular. Eles são entregues às aplicações usuárias à medida que são solicitados. Do ponto de vista do usuário contribuinte, nada foi alterado, ele continua a portar apenas o seu CI, como já ocorre atualmente com o e-CPF.

Nesta situação é desnecessária a manutenção de uma LCAR, simplificando a infraestrutura.

7.2.3.3 Legalidade

Não há diferenciação no aspecto legal da proposta se comparado ao sistema atual. Em ambas as situações, a legalidade é garantida pela lei que valida a assinatura digital efetuada por um CI da ICP-Brasil.

7.2.3.4 Interoperabilidade

Uma vez que o formato de CA e o próprio atributo são padronizados, as possibilidades de uso e reuso destes certificados aumentam bastante. Desta forma, supõe-se que este fato traria vantagens com relação à interoperabilidade. Entretanto, comparativamente com o sistema atual, o modelo proposto não traz diferenças significativas, uma vez que o atributo “CPF” já é padronizado (bem definido no formato e no local de preenchimento) e está presente no e-CPF.

Com relação à interoperabilidade do CI, ressalta-se apenas que os sistemas da RFB poderiam aceitar qualquer CI (no âmbito da ICP-Brasil) no seu processo de autenticação. Atualmente, apenas os e-CPFs são aceitos.

7.2.4 Outras análises específicas da proposta

Nesta seção são apresentadas outras análises específicas da proposta.

7.2.4.1 Vínculo à entidade

Conforme apresentado na proposta, a sugestão de um campo vinculante que possibilite a identificação de uma pessoa é o RIC e embora ainda não exista uma definição do formato, a sugestão é que ele seja informado no CI no campo *Subject.*

O ideal é que não ocorram alterações substanciais no formato do atual CI da ICP-Brasil, objetivando o máximo de compatibilidade com o atual perfil.

O campo *Holder* do CA deve ser preenchido com o RIC (sugerido na seção 4.3) usando a opção *entityName* (FARRELL et al, 2010).

Este tipo de vínculo é chamado de estrutura autônoma, conforme apresentado na seção 3.6.2 (PARK, 2000) e está representado na Figura 14.

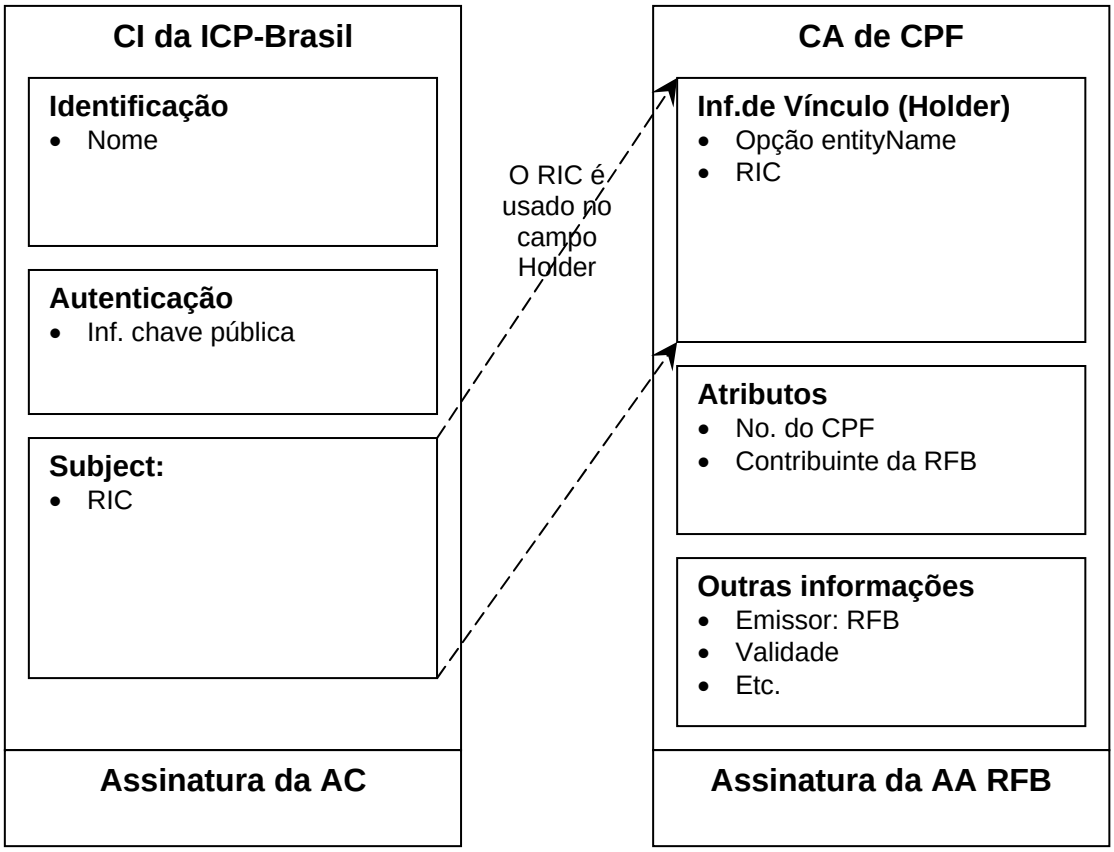

Figura 14 - Vínculo do CI com o CA de CPF

Fonte: elaborado pelo autor (2010)

7.2.4.2 Verificação da cadeia de confiança

No perfil atual do e-CPF, a verificação da cadeia de confiança é mais direta, pois é necessário a verificação do CI e-CPF do titular e dos certificados da ACs na cadeia de confiança até a AC Raiz da ICP-Brasil.

Na proposta com CA, a verificação é um pouco mais complexa, pois os sistemas verificadores do CA de CPF devem efetuar as seguintes tarefas para checar a autenticidade do CA:

a) verificar a cadeia de confiança do CI, como descrito anteriormente.

b) verificar a assinatura digital da RFB no CA. Esta assinatura deve ter sido realizada por meio do CI da AA que esteja no mesmo domínio de confiança do sistema verificador, ou seja, deve ter sido emitida por uma AC subordinada à AC-Raiz da ICP-Brasil;

c) verificar o vínculo entre o CI e o CA por meio do “RIC” contidos nos certificado conforme descrito na Figura 14.

7.2.4.3 Possibilidade de delegação

Para o atributo CPF, não existe a possibilidade de delegação no sistema atual e tampouco na proposta, uma vez que o portador não poderia assumir as funções da RFB na delegação do atributo CPF.

7.2.5 Exemplos de aplicabilidade

O mesmo formato de CA apresentado neste estudo de caso poderia ser utilizado nos seguintes atributos:

- título de eleitor;
- carteira nacional de habilitação;
- certidão negativa de débitos;
- certidão de situação civil.

A diferença que vai existir entre as aplicações citadas é a existência ou não de mecanismos de revogação, que são definidos em função do prazo de validade do certificado e o método de emissão do CA, se por meio do método *“push”* ou do método *“pull”.*

Em aplicações como “certidão negativa de débitos” ou “certidão de situação civil”, podem-se adotar prazos de validades curtos (de algumas horas), eliminando a necessidade de manter uma LCAR.

7.2.6 Conclusão

Neste estudo de caso, foi apresentada uma análise do uso da tecnologia de CA nas situações em que já existe um processo eletrônico existente por meio de CI no qual o atributo faz parte do certificado.

Os problemas do perfil atual do e-CPF foram os seguintes:

a) incompatibilidade dos prazos de validade do CI e dos atributos;

b) existência de mais de uma fonte de autoridade para um mesmo certificado.

Na proposta, emitem-se dois certificados: um de identidade e outro de atributo, vinculados logicamente por meio de um campo que identifica a pessoa (identificador sugerido é o RIC).

As vantagens da proposta são as seguintes:

a) a simplicidade de se montar uma IGP na comparação de uma ICP;

b) a possibilidade de outras entidades usarem esta tecnologia sem perda de segurança. A complexidade de uma ICP é conhecidamente alta e deve ser usada estritamente pelas aplicações para prover segurança ao processo de identificação e não para a qualificação do usuário e a definição dos seus privilégios;

c) a possibilidade de suportar a independência dos prazos de validades dos CIs e dos atributos. Os CIs e os CAs têm prazos de validades distintos e, portanto, não deve haver qualquer dependência entre eles;

d) a possibilidade de separação dos certificados de acordo com as suas respectivas fontes de autoridade. Elimina-se a necessidade atual do e-CPF de ter duas autoridades distintas no mesmo certificado ou uma autoridade com duas funções distintas (a AC emitente deve ser subordinada à AC-raiz da ICP-Brasil e simultaneamente de AC da RFB).

A urgência das entidades de prover alguma forma de mecanismos confiáveis de autenticação e definição de privilégios, aliado ao desconhecimento da tecnologia dos CAs, levaram a RFB à adoção de um CI com o atual formato do e-CPF que, conforme apresentado por este estudo, possui problemas que podem ser resolvidos por meio da tecnologia de CAs, sem perda de funcionalidade e de segurança.

8 ESTUDO DE CASO: E-CNPJ

Nesta seção, será apresentado o estudo de caso do uso CI e-CNPJ e a viabilidade de utilização de CA neste contexto.

O e-CNPJ é um certificado digital usado para garantir autenticidade e a integridade na comunicação entre a PJ e a RFB, funcionando exatamente como uma versão digital do CNPJ (CERTISIGN, 2009).

Com este documento digital é possível realizar consultas e atualizar os cadastros de contribuinte PJ, obter certidões da RFB, cadastrar procurações e acompanhar processos tributários por meio da Internet sem a necessidade de ir munido de diversos documentos até um posto de atendimento.

8.1 Sistema atual

A ICP-Brasil possui um certificado digital de Pessoa Jurídica (PJ) que define uma relação entre o titular (PF) e uma PJ. O e-CNPJ é um tipo específico de CI PJ no qual o titular é um dos responsáveis legais da entidade.

Na sua configuração atual, o preenchimento dos campos nome, CPF e data de nascimento do responsável pela PJ é obrigatório. Estes campos são preenchidos na extensão *SubjectAlternativeName*, dentro do campo *otherName*, sob os atributos:

a) OID 2.16.76.1.3.4 = nas primeiras 8 (oito) posições, a data de nascimento do responsável pela PJ, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o CPF; nas 11 (onze) posições subseqüentes, o número de inscrição no PIS/PASEP; nas 11 (onze) posições subseqüentes, o número do RG; e nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF (ITI, 2006);

b) OID 2.16.76.1.3.2 = nome do responsável pela pessoa jurídica (ITI, 2006).

O nome empresarial é obrigatório no e-CNPJ e deve ser incluído no campo *Subject* no formato *Distinguished Name (DN)* do padrão ITU X.500/ISO 9594*,* no subcampo *Common Name (CN)*. Este campo não pode ter mais do que 54 caracteres e não podem existir abreviações. Destes 54 caracteres, 49 são para o nome da empresa

acrescido do sinal de dois pontos (:) mais o número do CNPJ composto de 14 dígitos.

O e-CNPJ é um documento de propriedade da pessoa jurídica e que adicionalmente, identifica o representante legal da empresa junto à RFB (o representante tributário). Este representante tributário é indicado pela empresa, por meio dos seus representantes legalmente constituídos, para representá-la junto à RFB. O uso da chave privada da pessoa jurídica, por parte do representante tributário significa uma representação autorizada por ela e, sendo assim, deve responder pela prática dos seus atos, especialmente pelos atos realizados junto à RFB. Não é possível a geração de um e-CNPJ sem um representante legal ou com um representante legal que não tenha sido previamente atribuído pela empresa à RFB.

Quando se trata de assinar atos, independente da forma e da natureza, estes devem ser sempre realizados pela PF competente. Ou seja, mesmo que o ato seja para uma PJ, necessariamente a assinatura do ato é realizado por uma PF que tenha poderes legalmente constituídos para isto.

O fato de uma PF ser indicada como representante da PJ junto à RFB, não confere poderes ilimitados para ela agir em nome da empresa. Afinal, um contador não pode efetuar, por exemplo, compras ilimitadas em nome da empresa. Por outro lado, um dono de empresa não vai realizar por ele mesmo todas as transações eletrônicas do dia a dia de uma empresa.

Para ajudar a resolver o problema, a RFB disponibilizou no seu site na Internet a possibilidade de criar uma procuração eletrônica. Por meio deste mecanismo, o responsável pelo e-CNPJ da empresa pode delegar poderes para que outra PF ou PJ possa praticar atos perante a RFB em nome da empresa. Estes procuradores eletrônicos devem possuir um e-CPF ou um e-CNPJ.

Esta aplicação tem a sua eficiência limitada, pois foi criada para resolver o problema de procuração dentro dos domínios da RFB. Entretanto, esta solução não cobre todos os aspectos de delegação de poderes aos quais uma empresa realiza no seu cotidiano de operações. Existem outros domínios na empresa que também necessitam de mecanismos de procuração para que as pessoas possam executar e assinar atos em nome da PJ.

A tecnologia dos CA pode contribuir para fechar esta lacuna. Uma procuração eletrônica em formato de CA pode ser emitida pelos representantes legais da empresa e/ou pelos órgãos competentes às diversas PFs que necessitam desta procuração.

A gama de uso da tecnologia de CA nas empresas é bastante extensa. A seguir serão apresentados alguns cenários destes usos.

8.2 Relações associadas à constituição de uma empresa

Nesta seção serão descritos os procedimentos necessários para a abertura de uma pequena empresa. O objetivo é apontar os potenciais pontos de aplicabilidade da tecnologia de CA no dia a dia das PJs.

Para uma pequena empresa exercer suas atividades no Brasil é preciso, entre outras providências, ter registro na prefeitura ou na administração regional da cidade onde ela vai funcionar, no estado, na RFB e na Previdência Social. Dependendo da atividade pode ser necessário, também, o registro na sua respectiva Entidade de Classe, na Secretaria de Meio-Ambiente e em outros órgãos de fiscalização (SEBRAE, 2008).

As principais entidades às quais a empresa deve obter algum tipo de alvará ou licença de funcionamento serão descritas a seguir.

8.2.1 Registro de Pessoa Jurídica

O registro legal de uma empresa é obtido na Junta Comercial do estado ou no Cartório de Registro de Pessoa Jurídica. Este passo é equivalente à obtenção da Certidão de Nascimento de uma PJ. A partir desse registro, a empresa existe oficialmente - o que não significa que ela possa começar a operar.

Para fazer o registro é preciso apresentar uma série de documentos e formulários que variam de um estado para o outro. O mais importante deles é o Contrato Social e nele devem estar bem definidos os seguintes itens:

a) Interesse das partes;

b) Objetivo da empresa;

c) Descrição do aspecto societário e a maneira de integralização das cotas.

Ainda na Junta Comercial ou no Cartório, deve ser verificada a existência de alguma outra empresa registrada com o nome pretendido.

8.2.2 Cadastro no sistema tributário federal - obtenção do CNPJ

O próximo passo é obter o CNPJ, ou seja, registrar a empresa como contribuinte da RFB.

Ao fazer o cadastro no CNPJ, é preciso escolher a atividade (código CNAE) que a empresa irá exercer. Essa classificação será utilizada não apenas na tributação, mas também na fiscalização das atividades da empresa.

8.2.3 Obtenção do alvará de funcionamento

Com o CNPJ cadastrado, é preciso ir à prefeitura ou à administração regional para receber o alvará de funcionamento. O alvará é uma licença que permite o estabelecimento e o funcionamento de instituições comerciais, industriais, agrícolas e prestadoras de serviços, bem como de sociedades e associações de qualquer natureza, vinculadas a pessoas físicas ou jurídicas. Isso é feito na prefeitura, na administração regional ou na Secretaria Municipal da Fazenda de cada município. Para a emissão deste alvará são necessários alguns documentos, dentre os quais destacam-se a consulta prévia de endereço aprovada e os laudos dos órgãos de vistoria, quando necessários.

8.2.4 Cadastro no sistema tributário municipal

O cadastro no sistema tributário municipal deve ser feito junto à Secretaria de Finanças do município e ela deve ser feita pelas empresas prestadoras de serviços, pois o imposto sobre serviços (ISS) é de competência municipal.

8.2.5 Cadastro no sistema tributário estadual

O cadastro no sistema tributário estadual deve ser feito junto à Secretaria Estadual da Fazenda. Atualmente, a maioria dos estados possui convênio com a RFB, o que permite obter a Inscrição Estadual junto com o CNPJ, por meio de um único cadastro.

A Inscrição Estadual é obrigatória para empresas dos setores do comércio, indústria e serviços de transporte intermunicipal e interestadual. Também estão incluídos os serviços de comunicação e energia. Ela é necessária para a obtenção da inscrição no ICMS (Imposto sobre Circulação de Mercadorias e Serviços).

8.2.6 Cadastro na Previdência Social

O próximo passo é cadastrar a empresa na Previdência Social. Este cadastro ocorre nas agências regionais da Previdência Social. Após o cadastro, a empresa recebe o CEI (Cadastro Específico do INSS).

8.2.7 Aparato fiscal

Por último, deve-se preparar o aparato fiscal. Será necessário solicitar a autorização para impressão das notas fiscais e a autenticação de livros fiscais. Isso é feito na prefeitura de cada cidade.

8.3 Proposta: uso de CA nas relações associadas à constituição de uma empresa

Na seção anterior foram descritos os vários procedimentos necessários para a abertura de uma de uma pequena empresa. Nesta seção, será apresentado como o CA pode ser usado nestas situações.

Nesta proposta, criou-se hipoteticamente o estado “provisório” para o CNPJ. Desta forma, a primeira providência para a abertura da empresa, seria a obtenção de um CNPJ provisório que seria emitido pela AA RFB. O CNPJ seria então utilizado para fazer o vínculo dos CAs utilizados ao longo da proposta.

8.3.1 Registro na Junta Comercial ou Cartório de Registro de Pessoa Jurídica

A fonte de autoridade para a emissão deste CA é a Junta Comercial ou o Cartório de Pessoa Jurídica.

O empresário deve apresentar toda a documentação exigida e após a verificação da existência da duplicidade de nomes, a Junta Comercial ou o Cartório de Pessoa Jurídica emite um CA que atesta que a empresa está de acordo com todo o trâmite legal.

O vínculo entre o CA e a empresa deve ser feito pelo CNPJ provisório.

Existem algumas verificações obrigatórias que devem ser realizadas antes da abertura de uma empresa. As principais são as seguintes:

a) Emissão de Habite-se;

b) Certidão de registro na prefeitura (cadastro e lei de zoneamento);

c) Vigilância Sanitária do Município; se indústria e/ou comércio de alimentos ou de produtos ligados à saúde;

d) Vigilância Sanitária Estadual; se indústria alimentícia; comércio de produtos químicos em geral ou farmácias e drogarias;

e) Averbação do Contrato Social se a atividade exigir;

f) CETESB;

g) Secretaria Estadual do Meio Ambiente;

h) Corpo de Bombeiros;

i) Registro do Produto (Ministério da Saúde, representado pela Secretaria de Saúde do Estado);

j) SIF (Serviços de Inspeção Federal): Ministério da Agricultura;

k) Alvará de funcionamento de estabelecimento relacionado à Saúde na esfera municipal e estadual.

Nota-se que para cada um destes alvarás e verificações, é possível que seja emitido um CA. Nestas situações, sempre o campo vinculante entre o CA e a empresa será o CNPJ provisório.

8.3.2 Cadastro no sistema tributário federal - obtenção do CNPJ definitivo

A fonte de autoridade para a emissão do CNPJ é a RFB. O CNPJ é emitido por meio de um CA emitido para a empresa.

Atualmente a RFB emite o e-CNPJ para as pessoas jurídicas. Este certificado tem por objetivo identificar uma empresa e indicar que ela está devidamente inscrita na RFB como contribuinte. Além disso, o e-CNPJ indica também o responsável legal pela empresa.

Da mesma forma que o e-CPF, o e-CNPJ também mistura funções de qualificação e de identificação. Este perfil é chamado de centralizado (PERMIS, 2007) ou estrutura monolítica (PARK, 2000) conforme apresentado na seção 3.6.1. O registro de uma empresa como contribuinte é apenas uma qualificação da PJ e não deveria ser usado para identificá-la.

Nesta proposta, um CA de CNPJ é emitido para a empresa pela RFB, sem, no entanto, existir um vínculo a um CI. Este CA contém dados que identificam a empresa. Exemplo: razão social, endereço, um número seqüencial único emitido pela Junta Comercial ou Cartório de Pessoa Jurídica.

Outros CAs são emitidos pela RFB, entretanto nestes certificados o campo vinculante é sempre o CNPJ da empresa e o motivo é dar compatibilidade à prática disseminada pelo mercado para a identificação inequívoca de uma PJ. Os CAs abaixo podem ser emitidos pela RFB:

a) para o tipo de atividade econômica da empresa, Classificação Nacional de Atividades Econômicas (CNAE), é emitido um outro CA. A prerrogativa de definir o tipo de atividade exercida pela empresa é da RFB, portanto, ela também será a fonte de autoridade deste atributo. O CNAE é uma tabela desenvolvida pelo Instituto Brasileiro de Geografia e Estatística (IBGE) em conjunto com a RFB e qualquer órgão público pode usá-lo para classificar as

empresas de seu cadastro (IBGE, 2002). A Figura 15 mostra um exemplo deste CA;

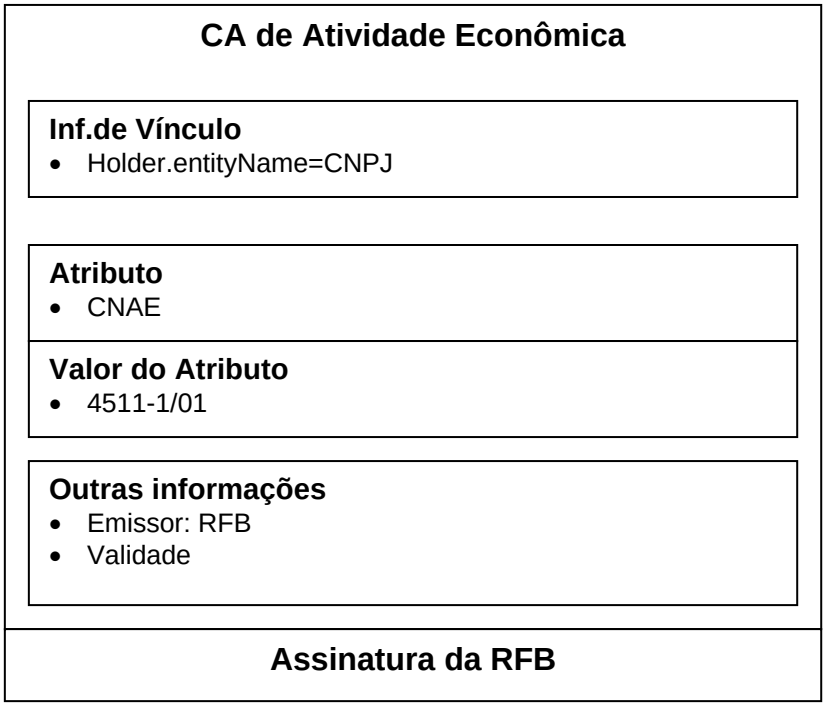

Figura 15 - Exemplo de CA de Classificação Nacional de Atividades Econômicas (CNAE)

Fonte: elaborado pelo autor (2010)

b) para o Quadro de Sócios e Administradores da empresa (QSA), também é emitido um CA, o qual contêm a relação dos nomes e respectivos CPFs dos responsáveis pela empresa. Além disso, também poderia ser emitido um CA para uma PF para qualificar seu papel legal dentro da PJ. A tabela das qualificações que uma pessoa física tem perante uma pessoa jurídica está bem definida pela RFB (RFB, 2010), o que facilitaria o uso deste tipo de CA. Este tipo de CA é apresentado com mais detalhes na seção 8.5.4;

c) para atestar a condição de ativo no CNPJ. Este CA pode ser usado também para efetuar a verificação do nome e endereço da empresa o que seria útil para os sistemas fora dos domínios da RFB. Este tipo de aplicação é análogo ao apresentado na seção 7.1 e tem alto potencial de uso e benefícios. A Figura 16 mostra um exemplo deste CA.

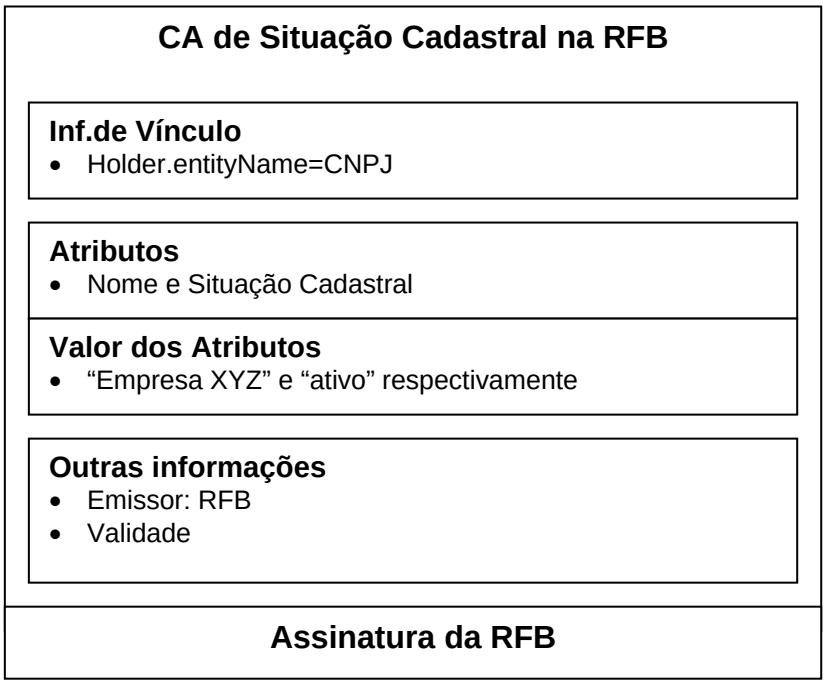

Figura 16 - Exemplo de CA de Nome e Situação Cadastral de uma empresa

Fonte: elaborado pelo autor (2010)

8.3.3 Obtenção do alvará de funcionamento

Após a obtenção do CA de CNPJ na RFB, a empresa necessita do alvará de funcionamento. Neste CA, a fonte de autoridade é a prefeitura e o emissor do CA pode ser a própria prefeitura ou as suas subsidiárias regionais. Este CA usa como campo vinculante o CNPJ, uma vez que a toda empresa deve ter o um CNPJ e é prática do mercado usar este campo como identificador único da pessoa jurídica. A Figura 17 mostra um exemplo deste CA.

A obtenção deste alvará pode estar vinculada à emissão de outros alvarás dos órgãos de vistoria e fiscalização, que por sua vez também podem ser emitidos na forma de CA. Abaixo alguns exemplos:

a) um alvará emitido pelo Corpo de Bombeiros, atestando as condições de funcionamento dos sistemas anti-incêndio;

b) um alvará da Companhia de Engenharia de Tráfego (CET) aprovando o impacto no trânsito local;

c) um alvará do Departamento de Controle de Uso de Imóveis (CONTRU) atestando a segurança do imóvel.

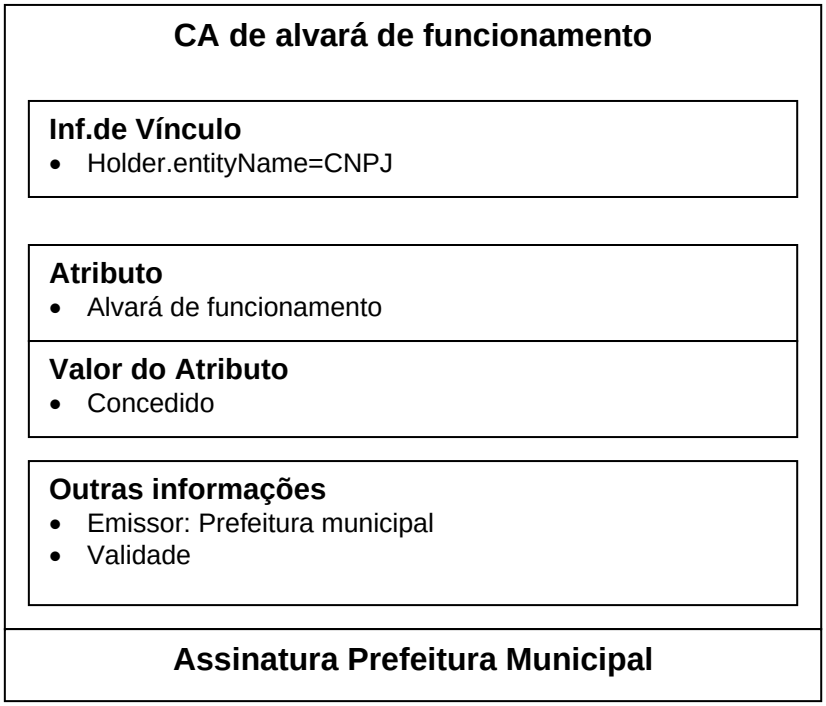

Figura 17 - Exemplo de CA de alvará de funcionamento emitido pela prefeitura do município

Fonte: elaborado pelo autor (2010)

8.3.4 Cadastro no sistema tributário municipal

A prefeitura também é a fonte de autoridade do atributo que atesta a inscrição da empresa prestadora de serviço no sistema tributário municipal. Este CA será usado para o recolhimento do Imposto Sobre Serviços (ISS) de competência dos municípios.

A empresa recebe um CA com um número de inscrição (em São Paulo é o Cadastro de Contribuinte Municipal - CCM). A Figura 18 mostra um exemplo deste CA.

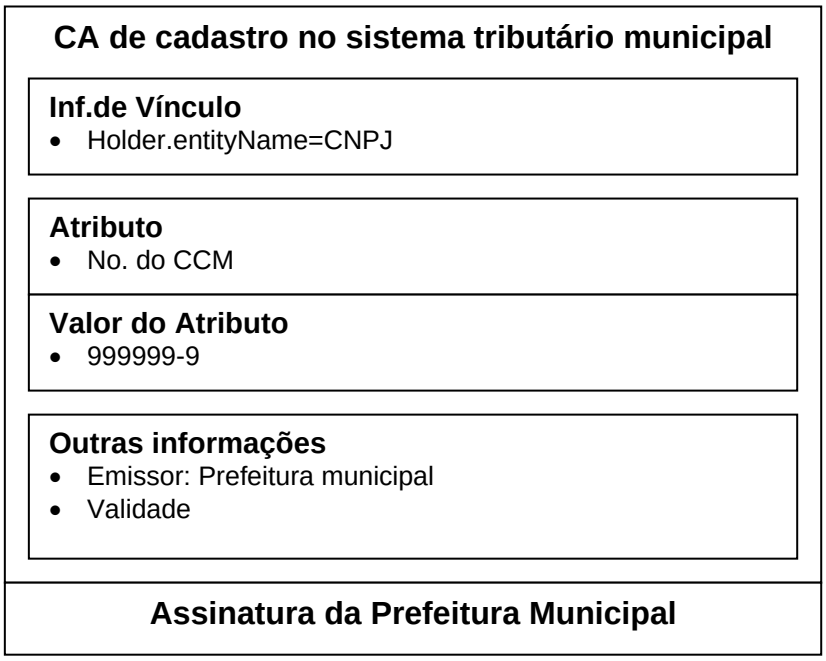

Figura 18 - Exemplo de CA de cadastro no sistema tributário municipal

Fonte: elaborado pelo autor (2010)

8.3.5 Cadastro no sistema tributário estadual

Os governos estaduais são as fontes de autoridade para a emissão do CA que atesta a inscrição da empresa no sistema tributário estadual, a chamada Inscrição Estadual. Este CA será usado principalmente para o recolhimento do Imposto sobre a Circulação de Mercadorias e Serviços (ICMS) de competência dos estados da federação. A Figura 19 mostra um exemplo deste CA.

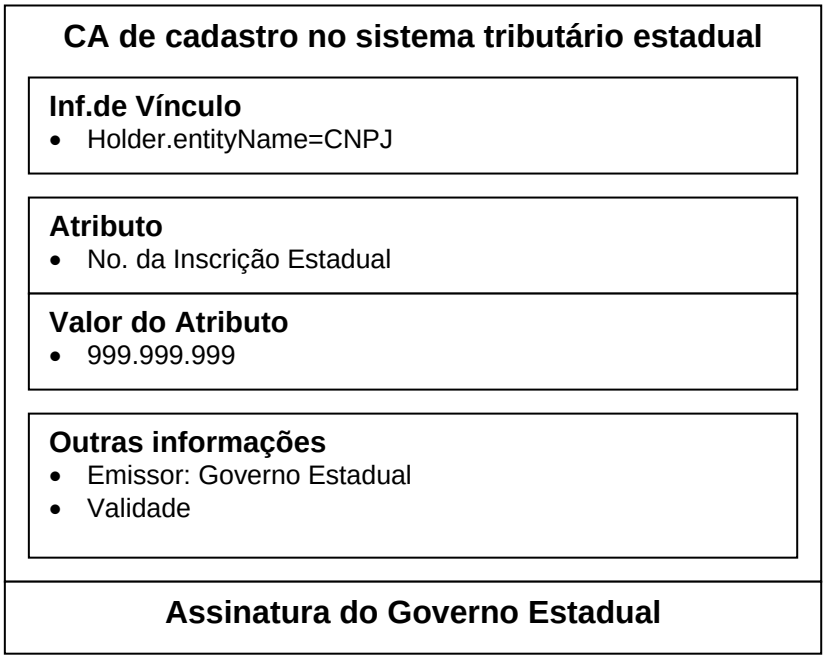

Figura 19 - Exemplo de CA de cadastro no sistema tributário estadual

Fonte: elaborado pelo autor (2010)

8.3.6 Cadastro na Previdência Social

A Previdência Social é fonte de autoridade para a emissão de CA que atesta a inscrição da empresa no Cadastro Específico do INSS (CEI). As subsidiárias regionais são as emissoras deste CA. A Figura 20 mostra um exemplo deste CA.

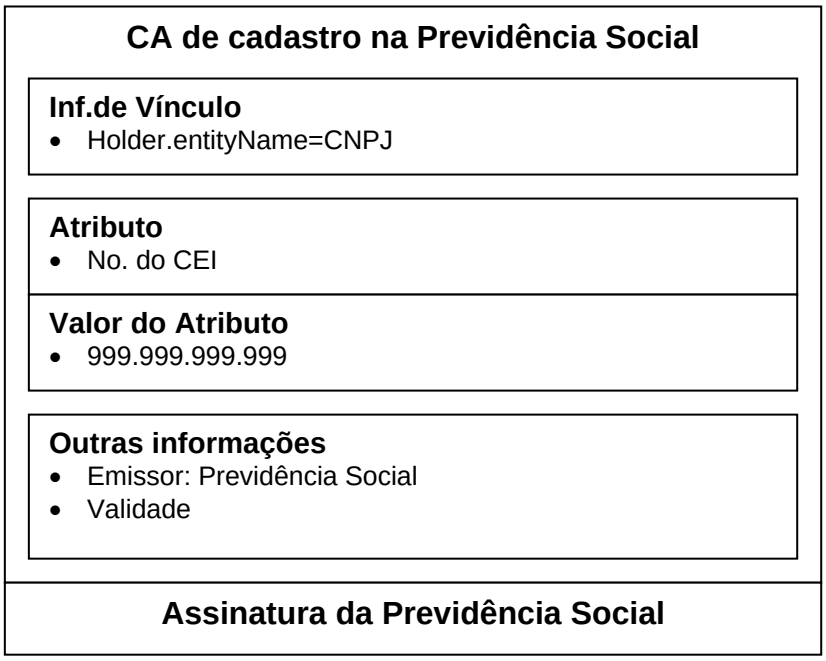

Figura 20 - Exemplo de CA de cadastro na Previdência Social

Fonte: elaborado pelo autor (2010)

8.3.7 Aparato fiscal

A prefeitura municipal é a fonte de autoridade para a emissão de um CA para a empresa, concedendo a permissão da impressão das notas fiscais (Figura 21).

A comprovação de que os livros fiscais foram assinados eletronicamente pela autoridade fiscal com sucesso, também pode estar em formato de um CA (Figura 22). Neste exemplo, ao invés de a autoridade fiscal realizar uma assinatura digital nos livros fiscais em formato digital, ela optou por emitir um CA para isto. Desta forma, houve a independência do meio físico que os livros fiscais foram emitidos, ou seja, estes livros podem ter sido emitidos digitalmente ou em formato analógico.

Este tipo de CA pode ser útil, pois nas situações de comprovação que os livros foram assinados pela autoridade fiscal, basta apresentar o CA. Sem a necessidade de apresentar todo o livro fiscal (digital ou papel) e a respectiva assinatura.

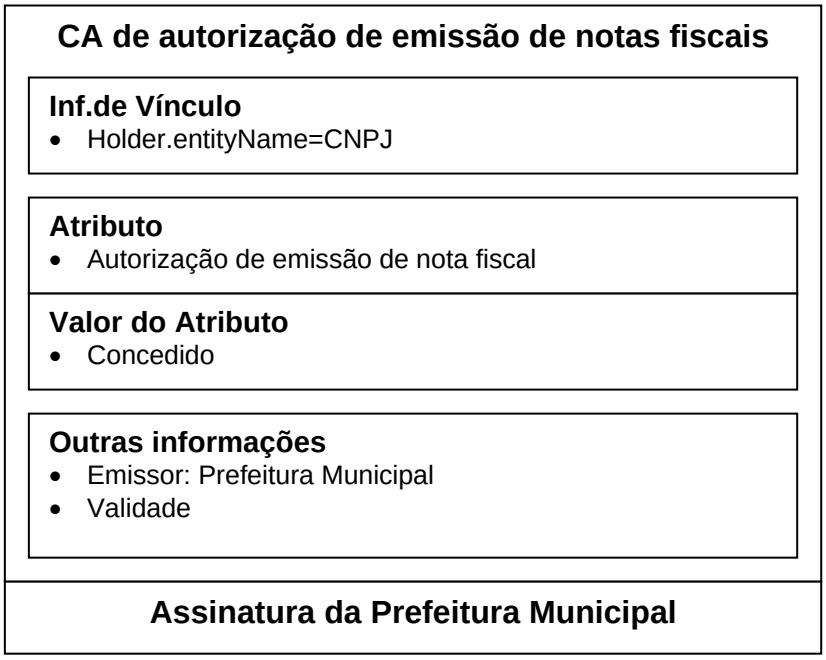

Figura 21 - Exemplo de CA de autorização de emissão de notas fiscais

Fonte: elaborado pelo autor (2010)

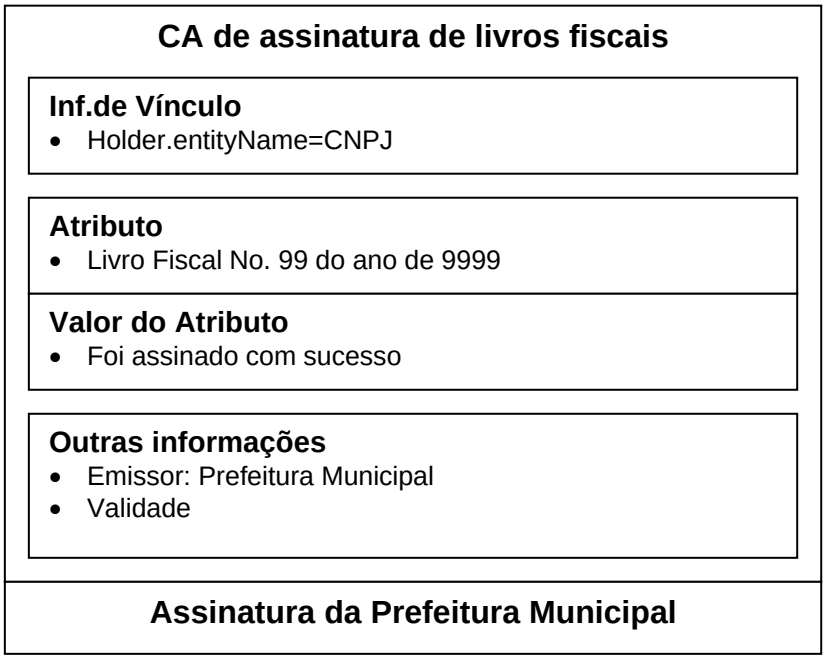

Figura 22 - Exemplo de CA de assinatura de livros fiscais

Fonte: elaborado pelo autor (2010)

8.4 Funcionamento destes CAs

Em todos os exemplos apresentados anteriormente, não houve a necessidade de um CI para a pessoa jurídica. Houve a necessidade de certificados de identidade, apenas nas situações que envolviam pessoas físicas. Isto ocorre, porque todos os CAs giram em torno de outros CAs.

8.5 Classes de aplicabilidade do CA para PJ

Nesta seção são apresentadas as classes de aplicabilidade do CA para a PJ.

a) vínculo da pessoa jurídica a uma entidade;

b) atribuição de estado da pessoa jurídica;

c) atribuição de papel da pessoa jurídica;

d) delegação de tarefas emitida pela responsável pela pessoa jurídica.

8.5.1 Vínculo da pessoa jurídica a uma entidade

Este tipo de CA será usado para vincular uma empresa a uma determinada entidade. O atributo é do tipo “Group” apresentado em FARRELL et al (2010).

Este CA é emitido para as empresas para indicar que ela está inscrita ou vinculada a uma determinada entidade fonte de autoridade de um atributo qualquer.

Exemplos deste tipo de certificado:

a) Inscrições nos sistemas tributários das esferas federais, estaduais e municipais;

b) Cadastro em sindicatos patronais.

8.5.2 Atribuição de estado da pessoa jurídica

Este tipo de CA será usado para atribuir um estado da pessoa jurídica. O atributo é do tipo “*Group*” apresentado em FARRELL et al (2010).

Exemplos deste tipo de certificado:

a) Alvarás e licenças de funcionamento;

b) Laudos técnicos;

c) Autorizações junto a órgãos reguladores;

d) Comprovantes de quitação de débitos fiscais (certidão negativa);

e) Comprovantes de pagamentos de impostos e taxas;

f) Comprovantes de situação cadastral.

8.5.3 Atribuição de papel da pessoa jurídica

Este tipo de CA é usado nos casos em que uma empresa assume um determinado papel ou função concedida por uma fonte de autoridade de atributo qualquer. O atributo é do tipo “*Charging Identity*” ou “*Role*” apresentado em FARRELL et al (2010).

Pode ser usado pela administração pública nas outorgas e concessões conferidas a empresas geralmente relacionadas à prestação de serviços. Exemplos deste tipo de certificado:

a) Outorga de serviços de telefonia fixa ou móvel;

b) Outorga de serviços de geração e distribuição de energia elétrica;

c) Contratos de concessão de administração de rodovias e cobrança de pedágio;

d) Atos de permissão, onde o estado transfere para as empresas permissionárias uma autorização temporária para a execução de um serviço (MEIRELLES, 1984).

Nas empresas privadas é usado nas situações em que uma pessoa jurídica fica subordinada a uma hierarquia no qual ela assume determinadas funções na estrutura de um complexo organizacional maior que é a fonte de autoridade do atributo. Exemplos deste tipo de certificado:

a) Concessionárias de veículos (fazem o papel de vendas e assistência técnica das montadoras);
b) Franqueados (fazem o papel de ponto de venda da franquia);
c) Postos de combustíveis (fazem o papel de ponto de venda das distribuidoras);
d) Distribuidoras de combustíveis (fazem o papel da distribuição das refinarias).

8.5.4 Atribuição do papel que uma pessoa física exerce na pessoa jurídica

Existem situações que é necessário a atribuição do papel que uma pessoa física exerce na pessoa jurídica. Nestas situações o CA pode ser emitido para uma PF com o objetivo de atribuir um papel, para que esta pessoa possa agir em nome de uma PJ, autorizado pelo responsável da empresa.

Exemplos deste tipo de CA:

a) contador (pessoa física) ou empresa de contabilidade autorizado a representar a empresa perante a RFB;
b) despachante aduaneiro (empresa ou pessoa física) autorizado a representar a empresa perante o Sistema Integrado de Comércio Exterior (SISCOMEX).

Aprofundando a análise do exemplo contador, o indivíduo que deseja se apresentar a um sistema como “contador da empresa XYZ”, deve apresentar inicialmente o seu CI para fazer o processo de autenticação. Após a autenticação, ele deve apresentar o CA de contador e na seqüência ele deve apresentar o CA de responsável da empresa XYZ. O conjunto destas credenciais lhe confere o papel de “contador da empresa XYZ”.

No caso específico do contador de uma empresa, existem duas alternativas para a geração dos CAs que definem esta credencial:

a) Utilizando Certificados de Identidade de Pessoa Jurídica (CIPJ);

b) Utilizando somente Certificado de Identidade de Pessoa Física (CIPF).

O próximo passo, de responsabilidade do sistema verificador, é verificar a autenticidade destas credenciais. Nesta fase, vários outros certificados auxiliam neste processo.

Nas situações descritas nas seções a seguir, todos os CIs (de PFs e PJs) são emitidos por uma AC da ICP-Brasil e o campo vinculante das PFs é o RIC.

8.5.4.1 Utilizando Certificados de Identidade de Pessoa Jurídica

Nesta seção é apresentado o processo de construção da credencial “contador da empresa XYZ”, a partir da emissão de CAs assinados por CIPJ. O exemplo deste tipo de CIPJ é o atual e-CNPJ. Neste tipo de CIPJ, o responsável pela PJ está explicitamente identificado no certificado.

Os passos abaixo descrevem os processos e os certificados correspondentes que são usados na verificação da credencial “contador da empresa XYZ”:

- Identificação da pessoa A:
    - CIPF de PA - Certificado de Identidade da Pessoa Física A;
- Qualificação do contador:
    - CA de contador: assinado com o Certificado de Identidade de Pessoa Jurídica do CFC
- Qualificação de contador da empresa XYZ:
    - CA de contador de XYZ: CA emitido pela pessoa B, responsável da empresa XYZ que qualifica a pessoa A como sendo “contador de XYZ”, assinado com o Certificado de Identidade da Pessoa Física B (CIPF de PB).
        - CA de responsável de XYZ: CA emitido pela Junta Comercial, assinado com o Certificado de Identidade da Pessoa Jurídica da

Junta Comercial que qualifica a pessoa C como responsável pela empresa XYZ e lhe confere poderes de definir o atributo “contador da empresa XYZ”.

A Figura 23 mostra os certificados envolvidos neste processo.

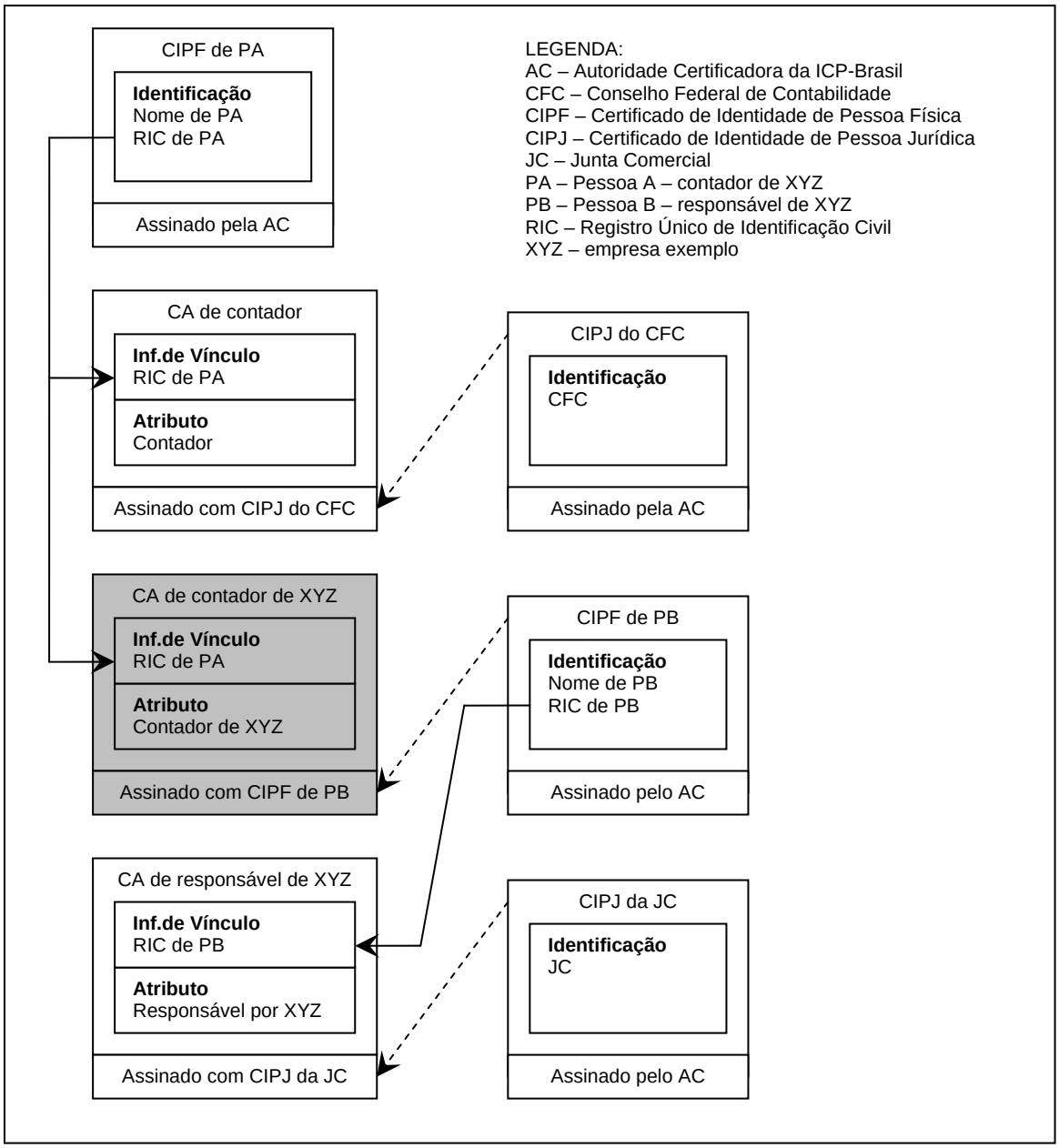

Figura 23 - Certificados necessários para a credencial "Contador da empresa XYZ" com CAs assinados pelo CIs de PJs (CIPJ)

Fonte: elaborado pelo autor (2010)

Neste cenário, a exemplo do que ocorre atualmente, existe a necessidade de um CI de PJ emitido por uma AC da ICP-Brasil para assinar o CA de contador emitido pelo CFC e o CA de responsável de XYZ emitido pela Junta Comercial.

Nos sistemas manuais em que não havia ainda os certificados digitais, não existia a possibilidade de uma pessoa jurídica assinar um documento. Sempre a assinatura era efetuada por uma pessoa física que detinha a prerrogativa legal para assinar pela empresa.

Os mecanismos que existiam e ainda existem para efetuar esta verificação é realizada com a verificação manual do contrato social (registrado na Junta Comercial) para a identificação dos sócios e representantes e as suas respectivas firmas reconhecidas por um cartório.

Com o advento dos certificados digitais, criou-se a possibilidade de uma pessoa jurídica efetuar assinaturas digitais. Este fato abriu uma lacuna na legislação, pois a legislação vigente sempre procurou cobrir os aspectos de assinaturas realizadas por pessoas físicas em nome de pessoas jurídicas.

Este vínculo entre pessoa física e pessoa jurídica está previsto no certificado digital. Entretanto, na prática ainda persistem problemas: para certificados de pessoa jurídica usado na autenticação de servidores não existem restrições, uma vez que o objetivo é autenticar uma sessão entre computadores e não realizar efetivamente uma assinatura eletrônica em um documento. Mas para assinar contratos, por exemplo, isto pode se tornar um problema. Pressupõe-se que o titular do CI de PJ tem o poder de realizar assinaturas em nome da PJ, mas não é verdade. O perfil de e-CNPJ atual define que o representante definido no CI de PJ é o representante perante a RFB apenas e não é a pessoa necessariamente qualificada para assinar um contrato por exemplo. Para este tipo de assinatura, a entidade que detém a prerrogativa legal de definir quais pessoas físicas podem assinar pela pessoa jurídica (podem existir várias, em conjunto ou individualmente, eventualmente com limitações de alçadas e poderes) é a Junta Comercial ou os Cartórios de Registro de Pessoas Jurídicas.

Este problema pode ser observado na Nota Fiscal Eletrônica (NF-e). As ACs têm emitido CIs de PJ com o uso específico para a NF-e. Neste tipo de certificado a pessoa designada como responsável não é necessariamente o mesma do e-CNPJ (se o fosse, seria o próprio e-CNPJ). O CI de PJ para NF-e é emitido para a pessoa designada pelo representante legal da empresa.

Conforme mencionado em SERASA (2010), um dos benefícios deste tipo de certificado são: “flexibilidade para emitir quantos certificados digitais forem necessários para atender à estrutura da sua empresa; e possibilidade de emitir o certificado digital para pessoas diferentes dos representantes legais registrados na Receita Federal do Brasil”.

Observa-se que o mercado continua no mesmo caminho de emitir CI com qualificadores. O e-CNPJ qualifica uma PF como representante da PJ perante a RFB e o CI de NF-e qualifica uma PF como responsável pela emissão de NF-e.

Na próxima seção é apresentado um cenário no qual são usados CAs para efetuar o vínculo entre a PF e a PJ.

8.5.4.2 Utilizando somente Certificado de Identidade de Pessoa Física

Nesta seção é apresentado o processo de construção da credencial “contador da empresa XYZ”, a partir da emissão de CAs assinados exclusivamente por CIPF. O exemplo deste tipo de CIPF é qualquer CI emitido no âmbito da ICP-Brasil.

Os CIs são dados apenas às PFs e o vínculo delas às PJs é realizado por meio de CAs.

Os passos abaixo descrevem os processos e os certificados correspondentes que são usados na verificação da credencial “contador da empresa XYZ”:

- Identificação da pessoa A:
    - CIPF de PA - Certificado de Identidade da Pessoa Física A;
- Qualificação do contador:

- CA de contador: assinado com o Certificado de Identidade de Pessoas Física da pessoa C, responsável pela CFC, ou especificamente responsável pela tarefa de assinar este CA do CFC.
    - CA de responsável pelo CFC: assinado pelo CIPJ do CFC que qualifica a pessoa C como responsável do CFC, ou especificamente concede o direito de emitir o CA em nome do CFC.

- Qualificação de contador da empresa XYZ:
    - CA de contador de XYZ: CA emitido pela pessoa B, responsável da empresa XYZ que qualifica a pessoa A como sendo “contador de XYZ”, assinado com o Certificado de Identidade da Pessoa Física B (CIPF de PB).
        - CA de responsável de XYZ: CA assinado com o Certificado de Identidade da Pessoa Física da pessoa D (CIPF de PD), responsável pela Junta Comercial, que qualifica a pessoa C como responsável pela empresa XYZ e lhe confere poderes de definir o atributo “contador da empresa XYZ”.
            - CA de responsável pela Junta Comercial: assinado pelo CIPJ da Junta Comercial que qualifica a pessoa D como responsável da JC, ou especificamente concede o direito de emitir o CA em nome da JC.

A Figura 24 mostra os certificados envolvidos neste processo.

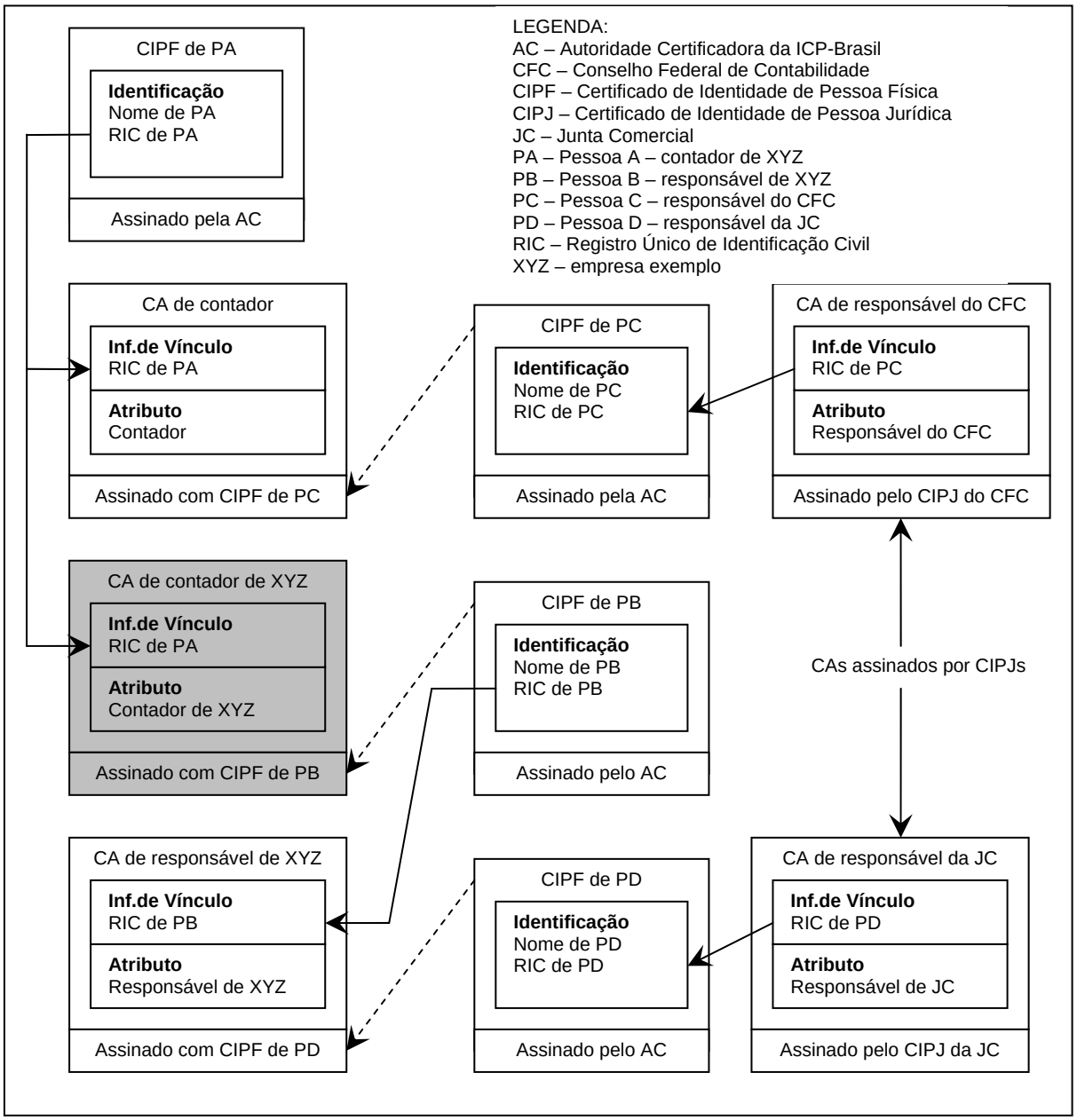

Figura 24 - Certificados necessários para a credencial "Contador da empresa XYZ" com CAs assinados pelo CIs de PFs responsáveis pelas PJs

Fonte: elaborado pelo autor (2010)

Uma das desvantagens deste cenário é a necessidade da existência de mais CAs para verificar as credenciais do titular “contador da empresa XYZ”, o que vai gerar uma carga maior de tarefas que os sistemas verificadores devem executar no momento de validar os CAs.

Comparado ao cenário anterior em que são usados CI para PJs, foram acrescidos os CAs que qualificam as PFs que assinam pelas PJs. Entretanto, observa-se também que sem os CIs de PJs, torna-se necessária a existência de CAs emitidos pelas AAs para as PFs assinarem CAs em nome da AAs: na Figura 24 estes certificados são o CA de responsável do CFC e o CA de responsável da JC.

A vantagem é a possibilidade de existirem mais de um responsável pela PJ (no e-CNPJ só é possível indicar um responsável pela PJ). Além disso, é possível também atribuir diversos papéis (não apenas o “responsável”) a estas PFs, tornando os mecanismos de delegação e atribuição de papéis mais flexíveis em comparação com o e-CNPJ atual.

Nota-se também neste cenário, que o CI de PJ ainda é necessário para assinar os CAs de responsáveis (ou papéis) da AA. Este CI deveria existir com este propósito específico a exemplo do que ocorre com os CIs das ACs. Neste tipo de CI (que é de PJ) não existe a figura do representante definido no certificado e o propósito é apenas de permitir a assinatura eletrônica de certificados digitais e das listas de revogação, conforme pode ser observado em um exemplo de CI de uma AC na Figura 25.

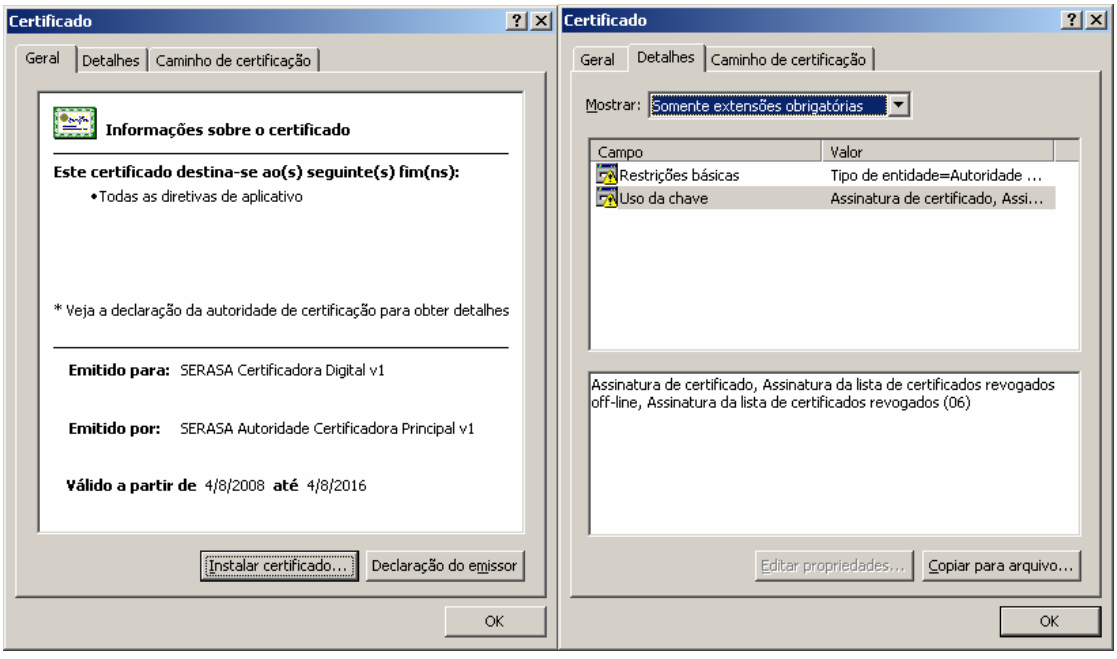

Figura 25 - Propósito do uso da chave de uma Autoridade Certificadora

Fonte: SERASA (2008)

Com a possibilidade da existência de CAs para a atribuição do papel que uma PF pode exercer em um PJ, faz-se necessário que os atributos sejam devidamente classificados em uma tabela para que os sistemas usuários possam identificá-los e atribuir o respectivo privilégio.

Para que os sistemas usuários sejam capazes de checar a veracidade do CA, é necessário verificar todos os certificados envolvidos no processo e para isto é importante que eles sejam apresentados ao sistema verificador.

Além disso, as regras de validação também devem ser bem definidas. Por meio destas regras, os sistemas usuários podem percorrer a cadeia de certificados e suas dependências para efetuar a validação.

8.6 Análise da proposta

Nesta seção são analisados a proposta de uso de CA para PJ e uso de CA pra a atribuição do papel que uma PF exerce na PJ.

8.6.1 Segurança

No modelo atual de atribuição de papel, vínculo a uma entidade e/ou estado de uma PJ, esta tarefa é realizada por meio da emissão de documentos em formato de papel. Este tipo de documento é facilmente passível de falsificação e de difícil verificação. No modelo proposto, a segurança é melhor, uma vez que para verificar a autenticidade do CA, basta checar a assinatura digital presente no CA realizada pela AA emissora.

No modelo atual de atribuição do papel que uma PF exerce na PJ a segurança é garantida pelo uso do CI de PJ. Comparativamente com a proposta, a segurança é equivalente, pois em ambos utiliza-se CIs para a identificação.

8.6.2 Gestão dos atributos e certificados

No sistema atual de atribuição de papel, vínculo a uma entidade e/ou estado de uma PJ, os atributos são administrados pelas várias entidades que possuem a prerrogativa que emitir os respectivos documentos em formato de papel.

Como atualmente este tipo de documento não é padronizado, cada entidade administra a emissão destes documentos da forma que lhe convém. Na situação proposta, os CAs são padronizados assim como os atributos. Esta característica confere à proposta uma uniformização para a gestão dos atributos, sem perder a prerrogativa legal de cada entidade de emitir o seu atributo.

Com relação ao uso de CA para a atribuição de papel exercido por uma PF na PJ, no modelo atual, pode-se atribuir papéis da PF diretamente no CI de PJ, de tal forma que seriam necessários tantos CIs de PJ quantos fossem os papéis que as PFs exercessem na PJ. O problema deste modelo é a necessidade de que a AC emissora do CI fosse também a AA, ou que ao menos houvesse um convênio entre as duas autoridades para que o atributo fosse colocado no CI com segurança.

Na proposta, como existe a independência entre o CI e os atributos, não existe esta necessidade. A AC emite o seu CI como já o faz atualmente, e a AA emite o CA com o indicação do papel que a PF exerce na PJ. Esta característica facilita a administração uma vez que CA não possui senhas (não há segredo) e podem trafegar livremente por meios eletrônicos sem a necessidade de criptografia.

Existem outras vantagens presentes na proposta com relação à independência dos prazos de validade e da revogação dos certificados já apresentados na seção 7.2 2ª Aplicação: atendimento eletrônico de Pessoa Física.

As fontes de autoridade e os atributos já são conhecidos e determinados, entretanto não são padronizados. Existe a necessidade de padronizá-los e este é uma dificuldade para a implementação da proposta.

8.6.3 Legalidade

Uma vez que os CAs são documentos assinados digitalmente por meio de um CI de âmbito da ICP-Brasil, significa dizer que é um documento que deve ser legalmente aceito.

Com relação às entidades que atualmente emitem os seus alvarás, certificados de vínculos à uma entidade e atribuição de estado da PJ, na proposta não há alteração desta prerrogativa. Ou seja, mantém se os direitos de cada entidade alterando apenas a forma de apresentação dos documentos de papel para o formato eletrônico padronizado de CA. Portanto, neste aspecto não há diferença.

Sobre a atribuição de papel da PF na PJ, a legalidade da proposta depende ainda da padronização e a regulamentação de papéis. Por exemplo, é necessário um dispositivo legal (uma lei, por exemplo) que defina que o atributo “contador” presente no CA, seja aceito pelos sistemas.

8.6.4 Interoperabilidade

Uma vez que o CA e o próprio atributo são padronizados, sistemas diferentes dos mais variados domínios podem fazer uso destes certificados nos seus processo de autorização.

Nos CAs de alvarás, certificados de vínculos à uma entidade e atribuição de estado da PJ, o processo atual tem uma interoperabilidade limitada, uma vez que os documentos em papel não podem ser facilmente duplicados e distribuídos como cópias fiéis. O documento precisa ser copiado e autenticado por um cartório (terceira parte confiável). No modelo proposto, os CAs podem ser copiados livremente para os repositórios de dados dos sistemas que necessitam destas credenciais nos seus processos de autorização.

Para a atribuição de papel “responsável pela PJ perante a RFB”, comparativamente com o sistema atual, o modelo proposto não traz diferenças significativas, uma vez que este atributo já é conhecido e padronizado, com seu local de preenchimento e formato bem definido no e-CNPJ. Ou seja, em relação à interoperabilidade do atual e-CNPJ e um CI de PJ mais um CA de “responsável pela PJ perante a RFB”, não

existem diferenças. Porém, com relação a outros CAs de atribuição de papel de uma PF perante uma PJ, qualquer sistema que necessite destas credenciais poderia fazer uso destes certificados.

Vale ressaltar que na proposta de atribuição de papel da PF na PJ, a retirada do atributo “responsável pela PJ perante a RFB” do CI de PJ, permitiria que este certificado pudesse ser utilizado nos processos de autenticação dos sistemas da RFB. Atualmente, apenas o e-CNPJ é permitido.

8.7 Conclusão

Este estudo de caso apresentou o uso do CA para as diversas relações que uma empresa está sujeita durante a sua abertura e ao longo da sua vida. Além disso, foi apresentado:

a) como os certificados de atributos podem definir de forma segura as relações existentes entre as pessoas jurídicas e as pessoas físicas;

b) como o CA pode ser usado para atribuição segura de vínculos entre PJ e outras entidades;

c) como o CA pode ser usado para a atribuição de um estado de uma PJ;

d) como o CA pode ser usado para a definição de um papel que a PJ desempenha;

e) os problemas existentes no atual e-CNPJ relacionados ao vínculo entre a PF e PJ;

f) a necessidade de se criar um CI de PJ com o propósito específico de assinar CAs.

9 ESTUDO DE CASO: PRONTUÁRIO ELETRÔNICO DE PACIENTE (PEP)

Neste estudo de caso, será apresentado o uso da tecnologia de CA na atribuição de papéis previsto no Nível de Garantia de Segurança (NGS2) do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) (SBIS/CFM, 2009a).

9.1 Introdução

Segundo LIU (2001) PEP é uma “coleção de informações que tem como principal objetivo descrever o prontuário do paciente em formato eletrônico de tal forma que os cuidados médicos fossem suportados nos mais variados locais e cenários. Estas informações podem incluir, mas não se limitam à demografia, dados biométricos, histórico de saúde, histórico familiar, medicamentos, alergias, observações e orientações de cuidados e tratamentos”.

Os objetivos de uma padronização para o PEP é permitir a troca de dados clínicos de pacientes entre sistemas heterogêneos, diferentes tipos de usuários e diferentes entidades. São muitos os benefícios que poderiam ser obtidos caso houvesse esta padronização do PEP. Normas e padronização para a armazenagem de registros médicos ao longo do tempo de vida pessoas podem contribuir para o correto diagnóstico e prognóstico a ser prescrito (LIU et al, 2001).

Segundo LIMA (2006, apud REZENDE, 2008), dentre os benefícios que podem ser obtidos, destacam-se: “acesso rápido aos problemas de saúde e intervenções atuais; acesso a conhecimento científico atualizado com conseqüente melhoria do processo de tomada de decisão; melhoria de efetividade do cuidado, o que por certo contribuiria para obtenção de melhores resultados dos tratamentos realizados e atendimento aos pacientes; e possível redução de custos, com otimização dos recursos”.

O Conselho Federal de Medicina (CFM), através da Câmara Técnica de Informática em Saúde e Tele-medicina firmou um convênio de cooperação técnica com a Sociedade Brasileira de Informática em Saúde (SBIS) com o objetivo de responder às indagações que têm recebido sobre a legalidade da adoção dos meios

eletrônicos para capturar, armazenar, manusear e transmitir os dados de atendimento de saúde de um indivíduo. O resultado atual deste convênio, que teve início em 2002, é o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) (SBIS/CFM, 2009a).

A definição de S-RES, conforme SBIS/CFM (2009), é “Sistema para registro, recuperação e manipulação das informações de um Registro Eletrônico em Saúde”.

Segue abaixo um breve histórico do que foi produzido por este convênio desde a sua criação:

a) em 2002 foram aprovadas as "Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico", que dispôs sobre o tempo de guarda dos prontuários, com o estabelecimento de critérios para certificação dos sistemas de informação além de outras providências;

b) em 2004 criou-se a 1ª versão do “Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES)”, que deu início ao processo de certificação de auto-declaração, no qual inexiste um processo de auditoria de certificação;

c) em 2007 aprovaram-se as “Normas Técnicas Concernentes à Digitalização e Uso dos Sistemas Informatizados para a Guarda e Manuseio dos Documentos dos Prontuários dos Pacientes, Autorizando a Eliminação do Papel e a Troca de Informação Identificada em Saúde”;

d) em 2008 terminou a fase de auto-declaração e iniciou-se efetivamente o processo de certificação com base em auditorias;

e) em 2009 foi publicada a versão 3.3 do documento “Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES)”.

Este manual define vários requisitos relacionados aos sistemas de saúde como:

a) padronização de um conjunto de regras, protocolos e características de processos relacionados à saúde;

b) definição de prontuário médico e a atribuição de responsabilidades para o correto preenchimento, regras de digitalização, guarda e manuseio das informações;

c) padronização da identificação dos agentes de saúde e seus usuários, por meio do Cadastro Nacional de Usuários do SUS e o Cadastro Nacional de Estabelecimentos e Profissionais de Saúde - CNES;

d) aderência ao padrão de Troca de Informação em Saúde Suplementar (TISS). É o padrão definido pela Agência Nacional de Saúde Suplementar (ANS) para registro e intercâmbio de dados entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde. O objetivo do padrão TISS é atingir a compatibilidade e interoperabilidade funcional e semântica entre os diversos sistemas independentes para fins de avaliação da assistência à saúde (caráter clínico, epidemiológico ou administrativo) e seus resultados, orientando o planejamento do setor;

e) definição do padrão de segurança necessário para garantir a integridade, autenticidade, sigilo e não repúdio.

Existem atualmente dois Níveis de Garantia de Segurança (NGS) que os sistemas podem ser certificados: NGS1 e NGS2.

A diferença básica entre o NGS1 para o NGS2 é que, no segundo, é necessário o uso de certificados digitais de identidade da ICP-Brasil para os mecanismos de assinatura e autenticação e é permitido a eliminação completa do papel (SBIS/CFM, 2009a, p.12). No NGS1 não se pode eliminar o papel e as assinaturas são realizadas de forma manuscrita (SBIS/CFM, 2009a, p.49).

Para um S-RES obter o NGS2 é necessário que o sistema atenda os requisitos do NGS1. No início de 2010 existiam apenas dois S-RES com a certificação NGS2 (SBIS/CFM, 2010). Este fato ilustra a dificuldade para as empresas conseguirem a certificação, assim como, o estágio embrionário da adoção dos certificados digitais de identidade nas transações eletrônicas dos sistemas de saúde.

Os requisitos de segurança de um S-RES são fundamentais para garantir a privacidade, confidencialidade e integridade da informação identificada em saúde. Uma das principais motivações do CFM ao participar deste processo de certificação foi o de garantir o sigilo profissional, ou seja, que o acesso à informação identificada só possa ser feito por pessoas autorizadas. Além disso, o CFM define, por meio de seu Código de Ética Médica, uma série de conduta de sigilo profissional que devem ser respeitadas para não violar dados confidenciais entre o médico e o paciente (CFM, 2010).

9.2 Sistema atual

Nos sistemas S-RES NGS2 é necessário o uso dos certificados digitais de identidade da ICP-Brasil. Estes certificados devem atender às normas da ICP-Brasil (NGS2.01) e são usados na assinatura digital de documentos (NGS2.02), no processo de autenticação (NGS2.03) e na assinatura eletrônica de documentos digitalizados (NGS2.04).

Observa-se que foi definido como “recomendado” o item “NGS2.02.06 - Propósito da assinatura e papel do signatário", ou seja, o tipo de comprometimento que o signatário assume no momento de firmar a assinatura digital e o papel do signatário (SBIS/CFM, 2009a, p.63). Isto se deve ao fato de que não existe ainda uma norma que defina e padronize os papéis que podem ser assumidos neste tipo de assinatura.

A possibilidade de informar o papel do usuário permite que no futuro este campo possa ser utilizado na concessão de privilégios.

Atualmente, como não existe a obrigatoriedade do preenchimento do campo, a concessão de privilégios é definida por um sistema que fica no banco de dados do S-RES. É neste banco de dados que está definido o papel de cada usuário e o respectivo acesso de cada papel (SBIS/CFM, 2009a, p.55). Este mecanismo de atribuição de papel é interno ao sistema, centralizando o modelo de autorização. Exemplo: uma enfermeira recebe um determinado nível de acesso devido ao papel que desempenha no hospital. Esta definição é dada a ela por entidades que não tem comprovadamente a prerrogativa de conceder o privilégio. Geralmente o setor de

Recursos Humanos pede ao administrador para que lhe conceda os privilégios de enfermeira.

A crítica que se faz é na impossibilidade de definir com segurança que um determinado acesso foi realizado indevidamente porque quem atribuiu os privilégios ao usuário não tinha prerrogativa legal para isto. A prerrogativa legal é o que define a responsabilidade do Conselho Federal de Enfermagem (CFE) na concessão do atributo “enfermeira”.

Em um PEP são várias as relações que podem existir entre os seus participantes. A Figura 26 apresenta algumas entidades que podem interagir com um PEP. Nesta ilustração observa-se a presença de entidades independentes entre si, cada qual com as suas necessidades específicas de acesso ao PEP. A definição das responsabilidades de cada entidade é descentralizada, necessitando que exista um modelo de autorização baseado neste formato. O modelo de definição de privilégio pode ser o proposto por ZHANG et al (2007), no qual a atribuição de papel ocorre de forma descentralizada, ou seja, diversas fontes de autoridade de atributos podem declarar que uma pessoa exerce um papel e os diversos sistemas heterogêneos podem usar estas credenciais para a liberação de acessos aos recursos do S-RES. Para que este mecanismo funcione adequadamente é necessário que os S-RES acreditem nestas fontes de autoridade de atributos.

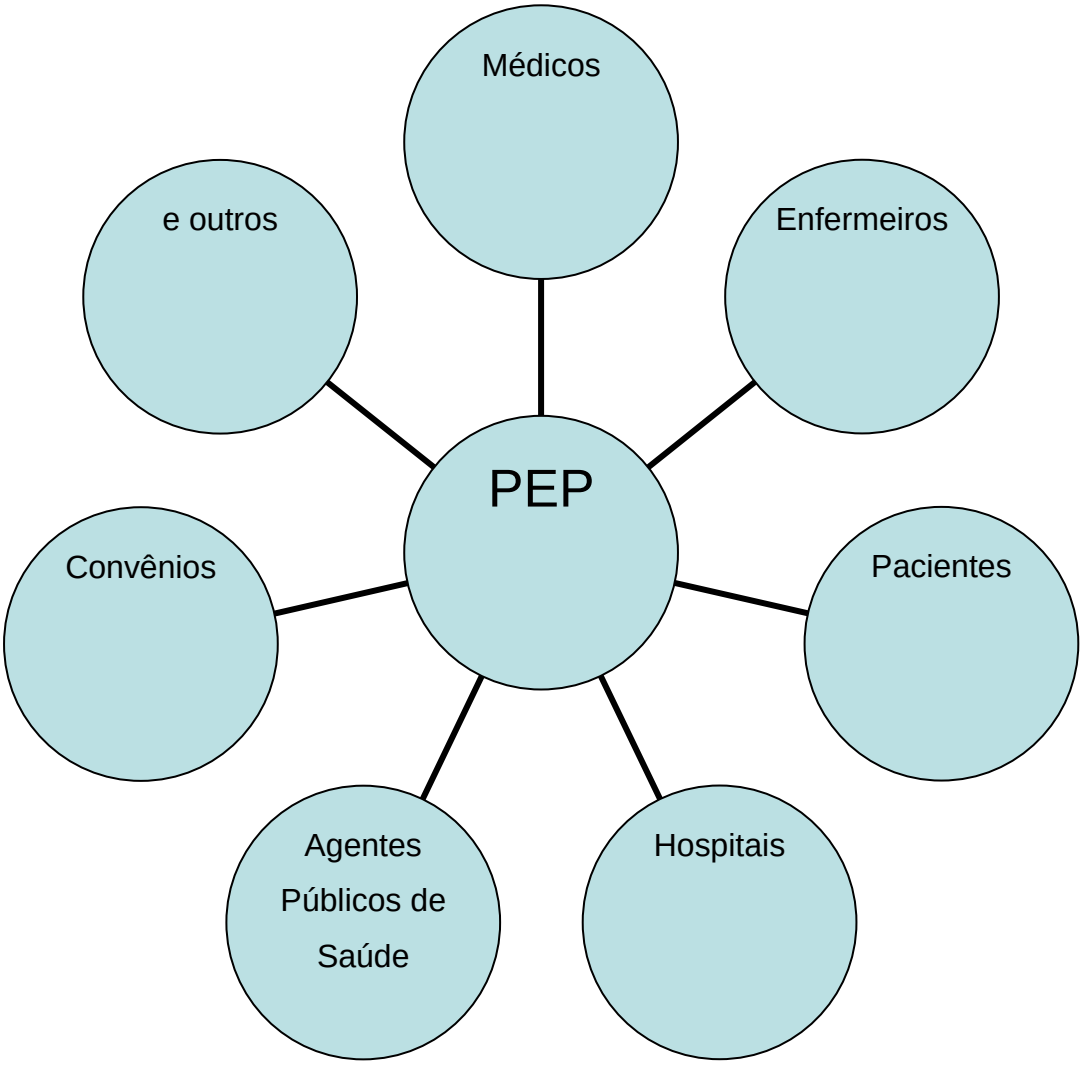

Figura 26 - Exemplos de entidades que interagem com um PEP

Fonte: elaborado pelo autor (2010)

A Figura 27 apresenta alguns componentes de um PEP. Todos estes componentes são recursos que precisam ser protegidos para garantir a privacidade do paciente (CFM, 2010). Entretanto estes recursos protegidos precisam estar adequadamente disponíveis de acordo com as necessidades de cada entidade que interage com o PEP, sem, contudo afetar a privacidade do paciente ou o Código de Ética Médica.

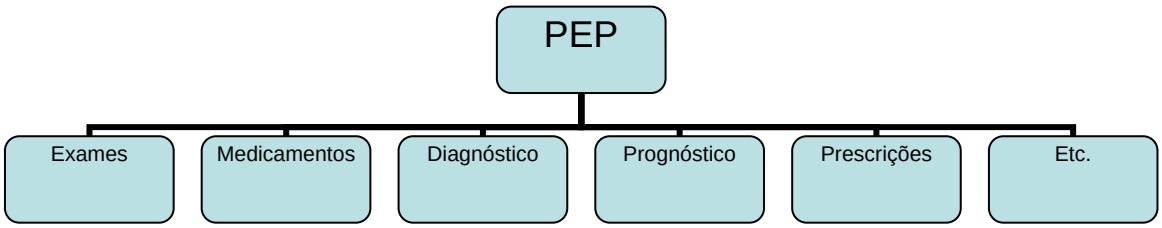

Figura 27 - Exemplos de componentes de um PEP

Fonte: elaborado pelo autor (2010)

9.3 Proposta

A proposta é apresentar um sistema que obedeça aos requisitos de segurança para o NGS2 e que cubra a lacuna existente de segurança com relação à definição de papéis dos usuários por meio da utilização de CA.

A necessidade de uso dos CIs da ICP-Brasil para os requisitos do NGS2 continua a mesma e, portanto do ponto de vista da segurança da identificação a proposta é a mesma.

A definição de papéis dos usuários será efetuada por meio da tecnologia dos CAs de forma que seja possível a incorporação de novas funcionalidades aos sistemas, uma vez que esta definição virá de fontes confiáveis e legais de autoridade de atributos.

No exemplo da “enfermeira”, este atributo é concedido por meio de um CA emitido pelo CFE. O vínculo entre o CA e a entidade (neste caso a pessoa) é dado pelo campo RIC (a exemplo do proposto na seção 4.3).

Desta forma, após o processo de identificação efetuado com o CI, o S-RES com NGS2, solicita o CA de enfermeira, verifica a sua veracidade por meio da assinatura digital do CFE e aceita o atributo “enfermeira” como parte das credenciais para a concessão dos privilégios.

Neste processo, outros CAs podem ser apresentados. Por exemplo, o CA que comprova o vínculo empregatício da pessoa com o hospital. A junção dos diversos CAs, alguns emitidos por entidades externas e outros emitidos por entidades internas, compõe o perfil final do papel do usuário e é um dos componentes do sistema verificador de privilégios do S-RES.

Outro componente que deve ser observado são as políticas de controle de acesso que são definidos em cada objeto protegido (ZHOU, 2003). Nestas políticas são definidos:

a) os domínios que o usuário tem direito de acesso;
b) a hierarquia de papéis e as suas relações entre si;
c) as FAAs dos atributos (papéis);
d) os parâmetros da delegação caso exista;
e) os domínios válidos da política de controle de acesso;
f) as ações possíveis de serem executadas;
g) e os papéis autorizados a executar uma ação em um objeto.

Após a avaliação destes itens, o sistema verificador tem condições de montar o privilégio resultante ao usuário.

9.3.1 Exemplo de funcionamento da proposta

Para descrever o funcionamento dos CAs nos S-RES foram usados exemplos de scripts de certificação da SBIS/CFM (2009b).

9.3.1.1 Exemplo: script NGS1.S009

A Figura 28 mostra o script usado neste exemplo.

NGS1.S009	NGS1.04.03 - Gerenciamento de usuários	**PR: 1)** Acessar com o usuário administrador e criar os seguintes usuários: **Maria Esteves** **Marco Rossi** 2) Atribuir os seguintes papeis aos usuários recém criados (caso não existem criá-los): Maria Esteves: **Recepcionista** Marco Rossi: **Auditor** Manoel de Abreu: **Médico radiologista** e **Técnico em radiologia** 3) Criar os seguintes grupos e inserir os usuários no grupo(s): **Medico-1 (Carlos Chegas; Cristina Maoli)** **Medico-2 (José Mouro; Carlos Chegas)** **RE:** Deve ser possível criar os usuários, papeis e grupos conforme descrito.

Figura 28 - Script NGS1.S009

Fonte: SBIS/CFM (2009b, p.19)

9.3.1.1.1 Procedimento com CA para NGS1.S009

Os passos abaixo descrevem como seria realizado o script de certificação NGS1.S009 caso o CA fosse usado.

No procedimento 1, o administrador acessa o sistema, autenticando-se por meio do seu CI da ICP-Brasil.

No procedimento 2, os papéis: Recepcionista e Auditor são atribuídos aos usuários pelo administrador. Estes papéis poderiam também ser atribuídos por meio de CA , mas não foram sugeridos neste exemplo porque como são atributos exclusivos do domínio, podem ser definidos pelo próprio sistema.

Ainda no procedimento 2, o usuário Manoel de Abreu deve fornecer os seguintes CAs: CA de Médico emitido pelo CFM, CA de Radiologista e o CA de Técnico em radiologia, ambos emitidos pela Sociedade Brasileira de Radiologia (SBRad). Estes CAs podem ser apresentados a cada acesso efetuado pelo usuário, ou por motivos de desempenho, podem ser armazenados no sistema para agilizar as definições de privilégios nos acessos subseqüentes do usuário.

No procedimento 3, os CAs dos médicos já devem estar presentes no sistema ou devem ser inseridos neste momento. Com estes CAs, o sistema permite que estes usuários possam ser alocados em grupos de médicos. Existe ainda a necessidade de que haja um mecanismo que informe ao sistema que apenas médicos podem fazer parte destes grupos (Médico-1 e Médico-2).

Tarefas de validação necessárias:

a) verificar se o CI apresentado pelo administrador foi assinado por uma AC da ICP-Brasil, conforme script NGS2.S001 (SBIS/CFM, 2009 p.30);

b) verificar se o CA de Médico foi assinado pelo CFM por meio de um certificado válido da ICP-Brasil;

c) verificar se o CA de Radiologista foi assinado pela SBRad por meio de um certificado válido da ICP-Brasil;

d) verificar se o CA de Técnico em radiologia foi assinado pela SBRad por meio de um certificado válido da ICP-Brasil;

e) verificar a validade, estado de revogação e integridade dos certificados, conforme script NGS2.S003 (SBIS/CFM, 2009 p.30).

9.3.1.2 Exemplo: script NGS1.S010

A Figura 29 mostra o script usado neste exemplo.

NGS1.S010	NGS1.04.05 – Configuração de controle de acesso	**PR:** Configurar o controle de acesso conforme descrito a seguir: 1) Recepcionista: **acesso a dados clínicos proibido** 2) Diretor administrativo: **acesso somente em leitura a dados clínicos** **RE:** Deve ser possível alterar os perfis de usuário atribuindo as permissões descritas.

Figura 29 - Script NGS1.S010

Fonte: SBIS/CFM (2009b, p.19)

9.3.1.2.1 Procedimento com CA para NGS1.S010

Os passos abaixo descrevem como seria realizado o script de certificação NGS1.S010 caso o CA fosse usado.

No procedimento 1, acesso a dados clínicos pela Recepcionista é proibido automaticamente, porque a Recepcionista não possui em suas credencias um CA emitido pelo CFM que permita este acesso.

No procedimento 2, o hospital emite um CA de “Diretor administrativo”. A lógica do sistema deve permitir a configuração de acesso de leitura de dados clínicos aos usuários com o papel “Diretor administrativo”.

Isto eleva a segurança do S-RES, transferindo completamente a responsabilidade desta definição ao hospital e CFM, sem depender de procedimentos manuais mais sujeitos a falhas.

Tarefas de validação necessárias:

a) verificar se o CI apresentado pelo gerente de segurança de sistemas foi assinado por uma AC da ICP-Brasil, conforme script NGS2.S001 (SBIS/CFM, 2009 p.30);

b) verificar se o CA de Diretor administrativo foi assinado pelo hospital por meio de um certificado válido da ICP-Brasil. Observar que o tipo de acesso concedido é somente leitura;

c) verificar a validade, estado de revogação e integridade dos certificados, conforme script NGS2.S003 (SBIS/CFM, 2009 p.30).

9.3.1.3 Exemplo: script NGS1.S016

A Figura 30 mostra o script usado neste exemplo.

NGS1.S016	NGS1.04.06 - Concessão de autorizações	**PR:** Sair do sistema e acessar como usuário Gestor de Segurança para verificar se há possibilidade de conceder autorização e definir controle de acesso para o usuário "Ângela Souza". 1 - Alterar o perfil do usuário de "Técnico de enfermagem" para "Enfermeiro" 2 - Sucessivamente entrar no S-RES com o usuário "Ângela Souza" e verificar se possui capacidade de cadastro de dados clínicos. **RE:** Deve ser possível para o Gestor de Segurança conceder autorizações e definir controle de acesso ao usuário de acordo com a necessidade

Figura 30 - Script NGS1.S016

Fonte: SBIS/CFM (2009b, p.22)

9.3.1.3.1 Procedimento com CA para NGS1.S016

Os passos abaixo descrevem como seria realizado o script de certificação NGS1.S016 caso o CA fosse usado.

No procedimento inicial, o usuário definido como “Gestor de Segurança” deve acessar o sistema, autenticando-se por meio de CI da ICP-Brasil. Em seguida conceder autorização e definir controle de acesso ao usuário “Ângela Souza”.

No procedimento 1, a alteração do perfil do usuário de “Técnico de enfermagem” para “enfermeiro” é realizado com a inclusão e exclusão no sistema dos CAs correspondentes.

No procedimento 2, são realizadas verificações sucessivas do tipo de acesso permitido. As concessões de autorização e a definição do controle de acesso do usuário são modificadas automaticamente de acordo com o perfil resultante dos CAs presentes no sistema.

Tarefas de validação necessárias:

a) verificar se o CI apresentado pelo gerente de segurança de sistemas foi assinado por uma AC da ICP-Brasil, conforme script NGS2.S001 (SBIS/CFM, 2009 p.30);

b) verificar se o CA de Técnico de enfermagem foi assinado pelo CFE por meio de um certificado válido da ICP-Brasil;

c) verificar se o CA de Enfermeiro foi assinado pela CFE por meio de um certificado válido da ICP-Brasil;

d) verificar a validade, estado de revogação e integridade dos certificados, conforme script NGS2.S003 (SBIS/CFM, 2009 p.30).

9.4 Análise da proposta

Nesta seção é realizada a análise do modelo proposto.

9.4.1 Segurança

Nos S-RES atuais, como não existe a obrigatoriedade do preenchimento do papel, a atribuição dos direitos de acesso concedidos aos usuários é realizada por um subsistema integrado ao S-RES (SBIS/CFM, 2009a p.16). Independentemente do mecanismo de concessão de privilégio adotado, seja diretamente ao usuário, seja por meio do papel que o usuário desempenha na organização, esta concessão é efetuada pela solicitação do RH ao administrador do sistema. Isto é uma vulnerabilidade, pois podem ocorrer erros (propositais ou não) neste processo, pois a entidade que concede o privilégio não é a que detém a prerrogativa legal para isto, além do que esta tarefa é realizada manualmente no S-RES.

Na proposta, com o uso do CA, este aspecto é bastante melhorado na medida em que os atributos são entregues aos titulares por entidades confiáveis e acreditadas por lei.

Para exemplificar: a credencial de “médico” apresentada pelo usuário por meio de um CA emitido pelo CFM lhe confere um determinado direito de acesso. A função que usuário ocupa dentro do hospital, lhe confere outro direito de acesso (esta credencial geralmente não está em formato de CA, uma vez que é interno ao S-RES). A credencial “cardiologista” apresentada pelo usuário por meio de um CA emitido pela Sociedade Brasileira de Cardiologia (SBC) lhe confere outro direito de acesso. O conjunto das credenciais apresentadas define o privilégio de acesso resultante.

Este fato evita que ocorram acessos indevidos por usuários não qualificados, protegendo a privacidade do paciente. Além de transferir a responsabilidade da atribuição de papel (que atualmente é do administrador do S-RES) para quem de direito tem a prerrogativa para isto.

A padronização dos papéis contribui também para padronizar os acessos permitidos aos dados do PEP. No sistema atual, já existe uma definição de dados clínicos e dados administrativos (SBIS/CFM, 2009a), mas a ligação existente entre os papéis e estes dados é feita internamente ao S-RES. Na proposta, muitas destas ligações poderiam ser feitas pelas próprias AAs. Por exemplo: o CFE define que a enfermeira tem direito de acesso aos dados clínicos, mas não aos dados administrativos do PEP.

9.4.2 Gestão dos atributos e certificados

O mecanismo atual de gestão do atributo é centralizado no S-RES. É responsabilidade do RH ou do administrador do sistema a atribuição de todos os papéis e privilégios de cada usuário.

No NGS2 a única garantia é a identificação inequívoca do usuário. Como não há uma IGP, não existe garantia que a atribuição de privilégios ocorreu com sucesso. Falhas podem ocorrer desde a incorreta atribuição de papel definida pelo RH até a

atribuição de papel executada pelo administrador do sistema no subsistema de segurança do S-RES.

Na proposta, nem todos os atributos serão emitidos por fontes externas de AAs. Os atributos administrativos e de administração do sistema continuam a ser definidos diretamente no subsistema de segurança do S-RES, dispensando o uso de CA. Exemplos de papéis que serão gerenciados internamente ao S-RES: Recepcionista, Diretor administrativo, Gerente de segurança de sistemas, Paciente, Administrador de sistema, Operador de sistema e Operador de cópia de segurança.

Os atributos provenientes de fontes externas de autoridade são gerenciados pelas respectivas AAs, fazendo com que o modelo de atribuição de papel seja descentralizado. São as AAs que fazem a gestão destes atributos como a emissão, manutenção e revogação. Exemplos de papéis que serão gerenciados por fontes externas de AA: Médico, Oftalmologista, Clínico geral, Radiologista, Técnico em radiologia, Patologista clínico, Enfermeiro, Técnica de enfermagem e Farmacêutico-bioquímico.

É possível que um determinado papel de usuário seja definido baseado em um ou mais CAs. Exemplo: para o papel “Médico Oftalmologista” é necessário o atributo “Médico” emitido do CFM e o atributo “Oftalmologista” emitido pela Sociedade Brasileira de Oftalmologia.

Os papéis usados como exemplos foram extraídos do Manual Operacional de Ensaios e Análises para Certificação de S-RES (SBIS/CFM, 2009b).

Comparativamente com o sistema atual, a proposta facilita a administração dos atributos, uma vez que menos atributos serão controlados pelo S-RES. A transferência da administração dos atributos para as AAs externas ao S-RES, trás benefícios, uma vez que os mesmos CAs por ela emitidos poderão ser usados por vários S-RES. Outro benefício relevante é transformar em certificados digitais os atuais mecanismos de controles de atributos presentes nestas AAs, a exemplo do que foi apresentado na seção “6. Estudo de Caso: Certificação digital da OAB”.

Em contrapartida, na proposta, cria-se um sobrecarga adicional para o S-RES efetuar a validação dos CAs, além de depender de uma conexão de dados com as AAs, independentemente se a emissão dos CAs for sob demanda ou estiver contido

em um cartão inteligente. A emissão sob demanda necessita de uma conexão para o envio do CA e se o CA estiver em cartão inteligente, ainda assim, o S-RES necessita de uma conexão para verificar a LCAR.

9.4.3 Legalidade

A legalidade do uso de CA para os diversos atributos apresentados pela proposta é garantida pela mesma lei que criou os certificados digitais de identidade (BRASIL, 2001) e garantiu a legalidade das assinaturas eletrônicas efetuadas com este certificado.

Comparativamente ao sistema atual, a legalidade pode ser questionada, uma vez que a atribuição de papel é realizada manualmente pelo responsável pela segurança do S-RES. A designação do atributo continua sendo de cada AA, entretanto a inclusão desta informação no S-RES é realizada de forma insegura.

Na proposta apresentada, a prerrogativa legal de cada AA foi mantida, ou seja, não houve alteração legal neste sentido. A diferença só é verificada por causa da transformação de um processo manual em automatizado e mais seguro. Esta transformação melhora a legalidade na definição do acesso ao S-RES, na medida em que retira do gerente de segurança a responsabilidade da atribuição manual dos papéis dos usuários, transferindo esta responsabilidade para as AAs de direito.

9.4.4 Interoperabilidade

Os S-RES possuem a característica de serem distribuídos, ou seja, existem diversas fontes de autoridade de podem interagirem com os S-RES. Com o uso de CA padronizado bem como os atributos, cria-se a possibilidade de sistemas heterogêneos usarem estes certificados.

Como exemplo, o mesmo CA de médico emitido pelo CFM, pode ser utilizado em qualquer sistema que necessite desta credencial. A interoperabilidade não se limita apenas aos S-RESs. Outros sistemas (por exemplo, do Ministério da Saúde) podem usar estes certificados.

Comparativamente com o modelo atual no qual os papéis são definidos em cada domínio, as vantagens são importantes, uma vez que elimina a necessidade de atribuição de papel em cada sistema/domínio.

Com relação à interoperabilidade do CI, não há diferença, uma vez que na proposta não houve alterações deste certificado.

9.5 Outras análises específicas da proposta

Nesta seção são abordados alguns aspectos específicos da proposta.

9.5.1 Delegação de Tarefas

Existe situações em que é necessário permitir que uma entidade dê permissão para outra entidade atuar como sendo a primeira. A descrição detalhada do mecanismo de delegação com CA é descrita na seção 3.5.

Em um S-RES é bastante comum este tipo de situação. Por exemplo, no script NGS1.S017, deseja-se conceder o poder de inclusão de dados clínicos de um paciente a um enfermeiro. Esta atividade é permitida a médicos e proibida a enfermeiros. Atualmente esta concessão deve ser informada diretamente ao subsistema de segurança do S-RES.

Caso fosse utilizado o CA para este mecanismo, o médico responsável, emitiria um Certificado de Atributo de Delegação (CAD) delegando este poder diretamente ao enfermeiro. Neste cenário, há 2 certificados: o CA de médico emitido pelo CFM e o CAD emitido pelo médico para o enfermeiro e o preenchimento das extensões de delegação conforme a ITU-T (2000) presentes nos certificados ocorreriam da seguinte forma:

a) a extensão “*basic attribute constraints*” do CA de médico deve conter o valor lógico VERDADEIRO, que indica que o titular pode delegar o papel de médico. Desta forma o titular passa a exercer o papel de uma AA e pode delegar os seus privilégios. Além disso, o campo deve vir acompanhado por um número inteiro (*pathLenConstraint*) com o valor 0 (zero) que significa que

a AA (médico) pode emitir CA apenas para entidades finais (nenhuma delegação subseqüente é permitida).

b) A extensão “*delegated name constraints*” do CA de médico deve ser definida como não crítica e deve ser deixada em branco, uma vez que o médico desconhece as pessoas às quais ele pretende um dia delegar este papel. Caso esta extensão seja preenchida, apenas as pessoas listadas poderão receber a delegação deste médico.

c) A extensão “*acceptable certificate policies*” do CA de médico deve ser definido que apenas os certificados de identidade no âmbito da ICP serão aceitos para o processo de delegação.

d) A extensão “*authority attribute identifier*” do CAD deve indicar o CA de médico. O objetivo é possibilitar ao subsistema de segurança verificar se o privilégio solicitado provém de uma fonte de autoridade confiável. O subsistema verifica se o CA de médico é válido.

Existem outros campos que poderiam ser preenchidos para um aumento na segurança do processo de delegação. Estes campos poderiam determinar a tipo de operação (leitura/escrita), o sistema alvo, uma tarefa específica ou uma parte apenas do privilégio inicial. O processo de delegação não é um mecanismo simples. Na RFC 5755 (FARRELL et al, 2010) a delegação é citada, mas não é recomendado uso de cadeias de delegação.

9.5.2 Vínculo ao CI

Como visto na seção 4.3, o vínculo do CA ao CI sugerido é realizado pelo RIC. Esta forma de vínculo é mais adequada, pois não existe a obrigatoriedade de se vincular um determinado CI aos CAs usados no PEP. Qualquer CI aceito legalmente (sob normas da ICP-Brasil) e válido pode ser usado para fazer a identificação da pessoa, desde que possua em seu corpo o número do RIC.

9.5.3 Dificuldades da proposta

Uma das dificuldades da proposta é a falta de padronização dos atributos. Não existe ainda uma tabela codificada de atributos definidos e regulamentados com as suas respectivas FAA.

Esta definição é importante porque por meio dela os S-RESs podem identificar corretamente a atribuição dos papéis. Os S-RESs precisam ser capazes de identificar um determinado papel de um usuário para poder liberar o acesso a um recurso protegido. Os papéis denotam funções que descrevem a autoridade e a responsabilidade concedidas a um usuário para o qual um papel foi associado (SANDHU, 1996).

Outra dificuldade é a falta de regulamentação das FAAs. É importante que a FAA esteja bem definida para um determinado atributo. Caso contrário, o subsistema verificador de privilégios do S-RES não tem condições de checar se a credencial apresentada permite o acesso aos recursos. A Tabela 5 apresenta alguns atributos da área médica e suas possíveis FAAs.

Tabela 5 - PEP – possíveis atributos e respectivas FAAs.

Atributos	**Fonte de Autoridade de Atributo**
Médico	CFM
Enfermeiro	CFE
Cardiologista	SBC
Hospital	CNES ou a RFB por meio do CNAE
Convênio	CNES, RFB por meio do CNAE ou ANS
Poder Público	AC – ICP Brasil

Fonte: elaborado pelo autor (2010)

Apenas neste pequeno exemplo, observa-se que podem existir dúvidas sobre a FAA dos atributos. Exemplo: qual órgão tem a prerrogativa legal de afirmar que uma

empresa é um convênio? O Cadastro Nacional de Estabelecimentos e Profissionais de Saúde, a Receita Federal do Brasil por meio do Código Nacional de Atividade Econômica ou a Agência Nacional de Saúde? Esta definição é importante porque o sistema verificador de privilégios do S-RES precisa identificar se o emissor do CA tem a autoridade sobre aquele atributo. No protótipo apresentado por ZHOU (2003), este campo foi incluído em uma tabela como parte da política de controle de acesso. A definição inequívoca da FAA é uma das premissas para que um sistema distribuído de atribuição de papel funcione e esta definição depende de regulamentação jurídica.

Outro problema existente também na proposta é a falta de definição de formato de CA a ser utilizado. No Brasil, ainda não existe esta regulamentação, embora existam alguns estudos em andamento no ITI (ITI, 2008). Esta regulamentação é importante porque os S-RES precisam saber reconhecer as informações contidas nos CAs.

Falta também uma regulamentação sobre os níveis de acesso permitidos para cada atributo. Em sistemas distribuídos como o PEP, desenvolver um modelo de autorização distribuída e com controle de acesso baseado em papéis seria importante para viabilizar o uso em larga escala do PEP em instituições de saúde. Além disso, o sistema deve assegurar a privacidade do paciente e ser suficientemente flexível para tratar as exceções (MOTTA, 2001).

A definição dos níveis de acesso passa também pelos tipos de operações que podem ser executadas. No protótipo apresentado por ZHOU (2003), foram usados os seguintes tipos de operações: buscar, alterar, eliminar, incluir, criar e mostrar.

Para o PEP que usa o modelo de autorização baseado em papéis, deve ser considerada também a existência de uma hierarquia de papéis (SANDHU, 2000). Por exemplo: o papel “médico” herda privilégios do papel “enfermeiro”.

Estes problemas não são triviais e vão demandar ainda algum tempo para a sua solução. Após a solução destes problemas, o próximo passo é alterar o manual de certificação do S-RES, com a mudança no NGS2 ou a criação de outro NGS para que os S-RES passem a aceitar e tratar os CAs.

9.5.4 Novo código de ética do CFM

O novo código de ética do CFM foi publicado em 13 de abril de 2010 e trouxe algumas importantes contribuições para a relação médico-paciente. Dentre os principais motivos da sua elaboração destacam-se para este estudo de caso:

a) aumentar a confiança na relação médico-paciente;

b) atualizar-se perante as mudanças da sociedade e dos novos recursos tecnológicos.

Neste contexto, o uso do PEP e o aumento da segurança sugerido pela proposta neste estudo de casos, auxiliam no cumprimento do código de ética nos seguintes aspectos:

a) emissão de receitas pode auxiliar o médico para atender à obrigação de fazer uma letra legível (CFM, 2010, cap. 3, art. 11);

b) o paciente tem direito de obter cópia do prontuário médico (CFM, 2010, cap.10 , art. 88);

c) o prontuário deve conter os dados clínicos em ordem cronológica com data, hora, assinatura do médico (CFM, 2010, cap.10 , art. 87, parágrafo 1º);

d) o médico tem obrigação de manter o sigilo dos dados dos pacientes (CFM, 2010, cap 1, XI).

9.6 Conclusão

O PEP já é uma realidade para o Brasil, mas ainda estamos em um processo embrionário do ponto de vista dos níveis de segurança.

A exposição de dados sigilosos de pacientes deve se efetuada de forma bastante granular para garantir que apenas informações autorizadas possam ser acessadas pelos agentes de saúde. Ou seja, a definição dos níveis de segurança deve ser atribuída para cada dado presente no PEP.

O uso dos CIs da ICP-Brasil no NGS2 oferece uma garantia do ponto de vista da identificação do usuário, mas apenas este mecanismo de identificação não permite a

existência da granularidade dos níveis de segurança necessária a uma adequada implementação de um PEP.

O uso do modelo de autorização baseado em papéis previstos no NGS2 foi uma escolha certa para os próximos passos relacionados à segurança do PEP.

Neste contexto o CA surge como uma alternativa viável para a atribuição dos papéis dos usuários. Estes certificados quando usados em conjunto com os CIs da ICP-Brasil conseguem prover os níveis adequados de segurança do PEP. Os CIs fazem a autenticação segura e os CAs fazer a qualificação segura dos usuários.

A credibilidade do S-RES é um fator importante para a disseminação do uso do PEP. Os pacientes precisam ter garantias que a sua privacidade não será invadida. Neste contexto, os CAs contribuem para transferir a responsabilidade da definição dos atributos às entidades autorizadas e o impacto desta transferência é o aumento da segurança e conseqüentemente a credibilidade oferecida pelos S-RES.

A implementação total desta tecnologia ainda depende de um esforço grande de regulamentação dos papéis e as fontes de autoridade de atributo, mas apresenta-se como o futuro para a criação de um PEP mais seguro e confiável.

10 CONCLUSÃO

Pela necessidade de prover segurança aos sistemas, tanto relacionada à identificação quanto relacionada à qualificação do usuário, muitas entidades têm adotado a tecnologia de certificados de identidade com atributos nas suas infraestruturas. Isto tem ocorrido porque não existe um conhecimento disseminado da tecnologia dos certificados de atributo. Este trabalho reforça as vantagens da separação de uma infraestrutura específica para o mecanismo de autenticação (ICP) e outra específica para a qualificação (IGP).

Para a construção de uma IGP é utilizado o CA que é um tipo de certificado específico para designar qualidades ao titular. O CA foi usado com sucesso no projeto piloto PERMIS apresentado na seção 2.2.1 e têm sido utilizado até hoje na Espanha no *Ilustre Colégio de Abogados de Madri* (ICAM) para a segura atribuição do papel “advogado”. Estas situações reais reforçam o potencial de aplicabilidade desta tecnologia.

Para garantir que o processo de autenticação é necessário o uso de CI. Algumas aplicações que usam CA, não necessitam de CI. O CA deve ser vinculado ao titular e não ao CI. Este trabalho apresenta como sugestão o RIC como campo vinculante entre o CA e o titular pessoa física e o CNPJ como campo vinculante entre o CA e o titular pessoa jurídica. A escolha de um campo identificador único para o vínculo à entidade é importante para as aplicações e por isso foi sugerido neste trabalho.

Para a correta implementação da tecnologia de CA é necessária a escolha do tipo de atributo que mais se adéqua ao perfil da aplicação. Para isto foram apresentados os diversos estudos de caso, os quais englobam os perfis de uso mais comuns.

O Estudo de Caso: Certificação digital da OAB propõe a criação de uma IGP para o atributo “advogado” em substituição da atual ICP-OAB, com a análise desta proposta. Este tipo de CA pode ser utilizado por qualquer tipo de entidade de classe que necessite identificar entidades pertencentes a determinado grupo.

O Estudo de Caso: Cadastro de Pessoa Física (CPF) apresentou a aplicação “consulta nome e situação cadastral”, no qual propõe a substituição do sistema atual de consultas efetuadas diretamente ao site da RFB, por uma aplicação utilizando

apenas CAs (sem CIs). Esta aplicação é bastante usada por empresas e tem alto potencial de uso e benefício.

Além disso, este estudo efetuou uma análise dos problemas relacionados aos prazos de validade dos campos qualificadores e identificadores e os possíveis conflitos entre fontes de autoridade, decorrentes da junção em um único certificado de funções de identificação e qualificação, a exemplo do e-CPF.

Os dois perfis de emissão de CA: o "*pull*" e o "*push*" e a necessidade ou não da existência de mecanismos de revogação, também foram abordados por este estudo de caso.

No Estudo de Caso: e-CNPJ, o CA foi usado nas diversas relações que uma empresa está sujeita durante a sua abertura e ao longo da sua vida. Além disso, foi descrito como CAs podem definir de forma segura as relações existentes entre as pessoas jurídicas e as pessoas físicas. Este estudo propôs também que seja criado um CNPJ com estado provisório que seria utilizado como campo vinculante nos estágio iniciais da abertura da empresa e apenas mudaria de estado após o efetivo funcionamento da empresa. Desta forma, seria adotado o CNPJ em todos os CAs emitidos para pessoas jurídicas.

Além disso, foi analisado um cenário para a construção de uma credencial para a definição do papel que uma PF exerce sobre uma PJ. Esta análise sugere algumas alterações no e-CNPJ para que passe a suportar múltiplos papéis e não apenas um responsável, como é atualmente.

No Estudo de Caso: Prontuário Eletrônico de Paciente (PEP), o CA foi proposto para realizar a atribuição de papéis aos envolvidos no PEP. O CA foi incluído como um novo componente de segurança no processo de certificação dos Sistemas de Registro Eletrônico em Saúde definidos pela Sociedade Brasileira de Informática em Saúde e pelo Conselho Federal de Medicina. O PEP é o tipo de aplicação no qual a atribuição de papéis é tipicamente distribuída, no qual várias fontes de autoridade são envolvidas para a definição de um perfil de acesso. Adicionalmente, foi descrito o uso de CA na delegação de tarefas, com o objetivo de avaliar as possibilidades deste mecanismo com o uso dos CAs.

Uma das limitações deste trabalho refere-se à composição do campo vinculante entre CAs, CIs e entidades. A RFC 5755 (FARRELL et al, 2010) indica que o conteúdo do campo “*Subject*” do CI deve ser igual ao campo “*Holder*” do CA. Atualmente o campo “*Subject*” do CI é preenchido com várias informações como: o nome, local, país, CPF e outros. Algumas destas informações podem ser irrelevantes (ou não disponíveis) para o preenchimento do campo “*Holder*” do CA. Além disso, existem aplicações com CAs que dispensam o uso de CIs. O desafio é construir um campo “*Distinguished Name*” para ser preenchido no “*Holder*” do CA e no “*Subject*” do CI, de tal forma que o uso do CI não seja obrigatório.

10.1 Conclusão Final

Este trabalho contribui para disseminar este conhecimento e se agrega ao rol de trabalhos sobre um assunto de extrema relevância para o futuro dos certificados digitais.

Sobre a viabilidade da adoção desta tecnologia destacam-se os quesitos abaixo:

a) Segurança: é viável uma vez que o uso do certificado de atributo torna as aplicações mais seguras ou ao menos se igualam neste aspecto, além disso, CAs permitem facilmente a realização de verificações futuras de autenticidade;

b) Gestão dos atributos e certificados: a separação entre duas infraestruturas distintas, ICP e IGP, uma exclusiva para autenticação e outra para autorização produz benefícios na gestão dos certificados na medida em que facilita a sua administração;

c) Legalidade: é obtida porque já existe legislação que dá suporte aos certificados de identidade da ICP-Brasil e as suas respectivas assinaturas digitais. Nos estudos de casos, os certificados de atributos usados foram assinados por meio de certificados de identidade da ICP-Brasil, garantindo a legalidade do processo.

d) Interoperabilidade: é uma grande vantagem a padronização do formato dos CAs bem como os seus atributos. Esta característica confere uma grande

possibilidade destes certificados serem utilizados pelos mais diversos sistemas.

10.2 Contribuições

As contribuições deste trabalho são:

a) apresentar as vantagens e desvantagens da utilização de CA nos processos de autorização.

b) mostrar os benefícios do uso de CA e o salto qualitativo e quantitativo na oferta de serviços eletrônicos com o uso de CA, o que deve gerar retornos importantes para as empresas, pessoas e governos, na parte da oferta de serviços, uma vez que é uma tecnologia relativamente simples de ser adotada.

c) descrever as principais características da tecnologia dos CAs;

d) avaliar os benefícios desta tecnologia, por meio de análises comparativas de um ambiente com e sem a adoção dos CAs;

e) identificar os diversos cenários reais, nos quais é possível a implantação dos CAs;

f) descrever os mecanismos de emissão, revogação, formas de vínculo e delegação destes certificados, de forma a possibilitar a adoção do tipo adequado ao cenário;

g) verificar a adequação dos atuais certificados digitais da ICP-Brasil para que possam operar em um ambiente computacional com a presença dos CAs.

Esses resultados contribuem para uma melhor compreensão da interoperabilidade dos certificados de atributo e de identidade e, também, dos diversos cenários nos quais estas tecnologias podem ser aplicadas, não apenas no âmbito da ICP-Brasil, mas também em aplicações de outros contextos de ICP ou mesmo em aplicações de CAs sem vínculo a CIs.

10.3 Trabalhos futuros

Novos trabalhos poderão vir no futuro para completar e viabilizar o uso dos certificados de atributos apresentados nesta dissertação, tais como:

a) Um estudo sobre a padronização do formato e conteúdo dos certificados de atributos a ser adotado pela ICP-Brasil;

b) Um estudo para a definição da composição do campo vinculante entre os CIs, CAs e entidades, para o preenchimento do campo "*Subject*" do CI e o campo "*Holder*" do CA.

c) Um estudo para a definição e padronização das classes de aplicabilidade dos certificados de atributos que vierem a ser adotado pela ICP-Brasil;

d) Um estudo para a criação de um repositório nacional das fontes de autoridade de atributo de uso público. Necessidade apontada também em ARMINIO (2004).

REFERÊNCIAS

AASP. Associação dos Advogados de São Paulo. **Perguntas mais freqüentes**. Disponível em: <http://www.aasp.org.br/aasp/servicos/certdigital/c_faq.asp> Acesso em: 25 fev 2010.

ARMINIO, A.E. **Certificados de atributos, ¿el pariente pobre de las infraestruturas de clave pública ?** Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI), Espanha, no. 15, jul. 2004, p. 18-21.

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

BRASIL. **Medida provisória nº 2.200, de 28 de junho de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia e Informação em autarquia, e dá outras providências. D.O. Eletrônico**, Poder Executivo, Brasília, DF, 28 ago. 2001.

CERTISIGN – **e-CNPJ**. Disponível em: <http://www.certisign.com.br/produtos-e-servicos/certificados-digitais/e-cnpj>. Acesso em 06 dez 2009.

CFM. **Código de Ética Médica**. Disponível em < http://www.portalmedico.org.br/resolucoes/CFM/2009/1931_2009.htm>. Acesso em 20 jan 2010.

CHADWICK, D.W. **An X.509 Role-based Privilege Management Infrastructure.** Business Briefing: Global Infosecurity, 2002.

ETSI. EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **Eletronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates**. (ETSI TR 102 044 V1.1.1 2002-12). Disponível em :< http://portal.etsi.org/docbox/EC_Files/EC_Files/tr_102044v010101p.pdf>. França: DTS/ESI-000005, 2002.

FARRELL, S. et al. **An Internet Attribute Certificate Profile for Authorization**. RFC 5755. 2010.

GALLARDO, D. H. – **Apresentação realizada no 4º. Certforum – Fórum de Certificação Digital.** Brasília, 2006.

COOPER, D. et al. **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**. RFC 5280. 2008.

IBGE. **Manual de orientação da codificação em CNAE-Fiscal**. Secretaria da Fazenda do Estado do Paraná, subcomissão técnica para a CNAE - subclasses, vinculada à CONCLA - Comissão Nacional de Classificação. Set 2002.

ICAM - Ilustre Colegio de Abogados de Madrid. **Certificados de Atributos**. Disponível em <http://www.icam.es/certificadodigital/presentacion.jsp>. Acesso em: 09 jul 2007.

ICP-BRASIL – **Diretrizes da Política tarifária da Autoridade Certificadora Raiz da ICP-Brasil**. DOC-ICP-06. v.2.0. 18 abr.2006.

ICP-BRASIL – **Apresentação da ICP-Brasil**. Disponível em <https://www.icpbrasil.gov.br/apresentacao> Acesso em: 10 ago 2007.

ICP-OAB Infraestrutura de Chaves Públicas da OAB, **Perguntas mais freqüentes**. Disponível em: <http://cert.oab.org.br/info_dest.htm> Acesso em: 09 jul 2007.

ICP-OAB Infraestrutura de Chaves Públicas da OAB, **Fundamentos Jurídicos da ICP-OAB**. Disponível em: <http://cert.oab.org.br/fundam_jur.htm> Acesso em: 09 jul 2007.

ITI – **O que é certificação digital.** Disponível em <http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf>. Brasília, 2005.

ITI – **Resolução no. 42 de 18 de abril de 2006.** Aprova a versão 2.0 dos REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICPBRASIL, item 3.1.9.1. Documentos para efeitos de identificação de um indivíduo, Brasília, abr 2006.

ITI – **Perguntas freqüentes**. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/PerguntaQuarentaOito> Acesso em: 25 mai 2008.

ITI – **Perguntas freqüentes**. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/PerguntaDez> Acesso em: 25 mai 2009.

ITU-T Rec. X.509 ISO/IEC 9594-8, **The Directory: Authentication Framework**, mai, 1997.

ITU-T Rec. X.509 ISO/IEC 9594-8, **The Directory: Public-key and attribute certificate frameworks**, mar, 2000.

ITU-T Rec X.812 ISO/IEC 10181-3, **Security Frameworks for Open Systems: Access Control Framework**, 1996.

LIMA, A.F.C. **O processo de implementação do diagnóstico de enfermagem no Hospital Universitário da Universidade de São Paulo**. Revista da Escola de Enfermagem da USP vol.40 no.1. São Paulo. Mar 2006.

LINN, J.; NYSTRÖM, M. **Attribute Certification: An Enabling Technology for Delegation and Role-Based Controls in Distributed Environments.** ACM Press: Proceedings of the fourth ACM workshop on Role-based access control RBAC '99, out. 1999. p. 121-130.

LIU, G.C. et al. **Standards for the Electronic Health Record Emerging from Health Care's Tower of Babel.** Proceedings of the American Medical Informatics Association Symposium. NC. EUA. Pág. 388-392. 2001.

MARTINS, A. **Estudo e Implementação de Infraestrutura de Chaves Públicas com Aplicação em Controle de Acesso a Redes Sem Fio**. UFRJ. Rio de Janeiro. Mar 2004.

MEIRELLES, H. L, **Direito Administrativo Brasileiro**. Revista dos Tribunais. 10º edição, São Paulo, 1984.

MOTTA, G.H.B.; FURUIE S.S. **Um modelo de autorização e controle de acesso para o prontuário eletrônico de pacientes em ambientes abertos e distribuídos**. Revista Brasileira de Engenharia Biomédica, v. 17, n. 3, p. 141-150, set/dez 2001.

MYERS, M. et al. **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP**. RFC 2560. 1999.

OAB. **OAB de São Paulo expulsa 14 advogados este ano (2006)**. Disponível em <http://www.oab.org.br/noticia.asp?id=7381>. Acesso em 08 mai 2008

PARK, S. J e SANDHU R. - **Binding Identities and Attributes Using Digitally Signed Certificates.** Laboratory for Information Security Technology (LIST), George Mason University, EUA, 2000.

PERMIS - **PrivilEge and Role Management Infrastructure Standards Validation**. Disponível em: <http://www.permis.org/en/objectives.htm>. Acesso em 09 jul 2007.

POLK, W. et al. **Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.** RFC 3279. 2002.

REINALDO, D. F. **A ICP-Brasil e os poderes regulatórios do ITI e do Comitê Gestor**. Artigo publicado no Grupo de Resposta a Incidentes de Segurança da UFRJ, Rio de Janeiro, 2006.

REZENDE, Pedro Antonio Dourado de - **Certificados Digitais, Chaves Púbicas e Assinaturas - o que são, como funcionam e como não funcionam** – Disponível em <http://www.cic.unb.br/~pedro/trabs/cert.htm>. Acesso em 10 ago 2007. Universidade de Brasília, Brasília, 2000.

REZENDE, P.O.; GAIZINSKI, R.R. **Tempo despendido no sistema de assistência de enfermagem após implementação de sistema padronizado de linguagem.** Revista da Escola de Enfermagem da USP vol.42 no.1,São Paulo. Mar 2008.

RFB. - **Cadastro de Pessoas Físicas**. Disponível em <http://www.receita.gov.br/TextConcat/Default.asp?Pos=2&Div=GuiaContribuinte/CPF/>. Acesso em 14 mai 2008.

RFB. **Conceitos básicos**. Disponível em <http://www.receita.fazenda.gov.br/atendvirtual/Orientacoes/ConceitoBasico.htm#Certificado%20Digital%20e-CPF%20ou%20e-CNPJ>. Acesso em 27 mai 2008b.

RFB. **Perguntas e Respostas.** Disponível em <http://www.receita.fazenda.gov.br/PessoaFisica/CPF/PerguntasRespostas/PerguntasRespostas.htm#14> Pergunta no. 53. Acesso em 06 dez 2009a.

RFB. **Regularização de Situação Cadastral.** Disponível em <http://www.receita.gov.br/PessoaFisica/cpf/CPFRegularizacaoSitCad.htm>. Acesso em 17 dez 2009b.

RFB. **Tabelas Utilizadas pelo Programa CNPJ.** Disponível em < http://www.receita.gov.br/PessoaJuridica/CNPJ/tabelas/CodDesQSA.htm> Tabela de códigos e descrições de qualificações para o QSA e responsável perante o CNPJ. Acesso em 14 jan 2010.

SANDHU, R.S.; COYNE, E.J.; YOUMAN C.E. **Role-Based Access Control Models**, IEEE Computer, v. 29, n. 2, p. 38-47, fevereiro, 1996.

SANDHU, R.S.; FERRAIOLO, D. ; KUHN, R. **The NIST Model for Role-Based Access Control Towards A Unified Standard**. Proceedings of the fifth ACM workshop on Role-based access control. Berlin, Alemanha, 2000.

SBIS/CFM. **Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Registro Eletrônico de Saúde**. Versão 3.3. São Paulo, mai 2009a.

SBIS/CFM. **Manual Operacional de Ensaios e Análises para Certificação de S-RES.** Versão 1.2. São Paulo, mai 2009b.

SBIS/CFM. **Lista de Sistemas Certificados em NGS2.** Disponível em <http://www.sbis.org.br/site/site.dll/view?pagina=160>. Acesso em 17 jan 2010.

SALFORD; **Local e-organisation: Enablers**. Disponível em <http://www.salford.gov.uk/council/corporate/e-government/ieg/ieg2/ieg2organisation/ieg2-egov-enablers.htm>. Acesso em 09 jul 2007.

SEBRAE. **Guia prático para o registro de empresas.** Disponível em <http://www.sebrae.com.br/momento/quero-abrir-um-negocio/formalize-sua-empresa/registre/registro-de-empresas/14-guia-pratico-para-o-registro-de-empresas/BIA_14/integra_bia>. Acesso em 01 set 2008.

SERASA. **O que é um Certificado Digital para Nota Fiscal Eletrônica**. Disponível em <http://loja.certificadodigital.com.br/Serasa/SaibaMais/385/Certificado+Digital+para+Nota+Fiscal+Eletronica>. Acesso em 26 fev 2010.

TUECKE, S. et al. **Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile.** RFC 3820. 2004.

VILLAR, M.V.F. et al. **Segurança nos processos de Autenticação e Autorização através de certificados X.509.** São José dos Campos: SSI2004 – 6º. Simpósio Segurança em Informática, nov. 2004, artigo 3.

ZHANG X. et al. **A decentralized RBAC model and its user-role administration**. International Symposium on Communications and Information Technologies. Pág 1280 – 1285. 17-19 Oct 2007.

ZHOU, W; MEINEL C**. Implement Role-Based Access Control with Atribute Certificates**. FB IV-Informatik. Universität Trier, 54286, Trier. Alemanha, 2003.

REFERÊNCIAS CONSULTADAS

COSTA, C. G. A. **Desenvolvimento e avaliação tecnológica de um sistema de prontuário eletrônico do paciente, baseado nos paradigmas da World Wide Web e da engenharia de software**, Campinas, São Paulo, 2001. Dissertação (mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação, Campinas, São Paulo, 2001.

GUELFI, A. R. **Análise de elementos jurídico-tecnológicos que compõe a assinatura digital certificada digitalmente pela infraestrutura de chaves públicas do Brasil (ICP-Brasil)**, São Paulo, 2007. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos, São Paulo, 2007.

MAGALHÃES, M. A. **Análise Comparativa dos Modelos de Infraestrutura de Chaves Públicas**. São Paulo, 2005. 70 f. Trabalho de conclusão de curso – Especialista em Segurança de Sistemas e Redes de Computadores, Faculdade SENAC de Ciências Exatas e Tecnologia – Campus Santo Amaro, São Paulo, 2005.

APÊNDICE

A estrutura dos dados em um CA no formato X.509 na especificação ASN.1 é a seguinte:

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

AttributeCertificateInfo ::= SEQUENCE {
     version              AttCertVersion -- version is v2,
     holder               Holder,
     issuer               AttCertIssuer,
     signature            AlgorithmIdentifier,
     serialNumber         CertificateSerialNumber,
     attrCertValidityPeriod   AttCertValidityPeriod,
     attributes           SEQUENCE OF Attribute,
     issuerUniqueID       UniqueIdentifier OPTIONAL,
     extensions           Extensions OPTIONAL
}

AttCertVersion ::= INTEGER { v2(1) }
Holder ::= SEQUENCE {
      baseCertificateID   [0] IssuerSerial OPTIONAL,
                -- the issuer and serial number of
                -- the holder's Public Key Certificate
      entityName          [1] GeneralNames OPTIONAL,
                -- the name of the claimant or role
      objectDigestInfo    [2] ObjectDigestInfo OPTIONAL
                -- used to directly authenticate the holder,
                -- for example, an executable
}

ObjectDigestInfo ::= SEQUENCE {
     digestedObjectType  ENUMERATED {
             publicKey            (0),
             publicKeyCert        (1),
             otherObjectTypes     (2) },
                    -- otherObjectTypes MUST NOT
                    -- be used in this profile
     otherObjectTypeID   OBJECT IDENTIFIER OPTIONAL,
     digestAlgorithm     AlgorithmIdentifier,
     objectDigest        BIT STRING
}

AttCertIssuer ::= CHOICE {
     v1Form   GeneralNames,  -- MUST NOT be used in this
                             -- profile
     v2Form   [0] V2Form     -- v2 only
}

V2Form ::= SEQUENCE {
```

```
     issuerName            GeneralNames  OPTIONAL,
     baseCertificateID     [0] IssuerSerial  OPTIONAL,
     objectDigestInfo      [1] ObjectDigestInfo  OPTIONAL
       -- issuerName MUST be present in this profile
       -- baseCertificateID and objectDigestInfo MUST NOT
       -- be present in this profile
}

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

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

Attribute ::= SEQUENCE {
      type      AttributeType,
      values    SET OF AttributeValue
        -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType
```

Atributos padronizados

Alguns atributos foram padronizados pela RFC 5755 (FARRELL et al, 2010). Estes atributos seguem a formato abaixo:

```
IetfAttrSyntax ::= SEQUENCE {
     policyAuthority [0] GeneralNames    OPTIONAL,
     values          SEQUENCE OF CHOICE {
                       octets    OCTET STRING,
                       oid       OBJECT IDENTIFIER,
                       string    UTF8String
     }
}
```

Informação de Serviço de Autenticação

O atributo *SvceAuthInfo* identifica pelo nome o titular do CA para uma determinada aplicação. Geralmente este atributo conterá o par usuário/senha para aplicação legadas.

O formato deste atributo é mostrado abaixo e ele será criptografado, nos casos em que possuir informações sensíveis como uma senha por exemplo.

```
name      id-aca-authenticationInfo
OID       { id-aca 1 }
Syntax    SvceAuthInfo
values:   Multiple allowed

     SvceAuthInfo ::=    SEQUENCE {
          service   GeneralName,
          ident     GeneralName,
          authInfo  OCTET STRING OPTIONAL
     }
```

Identificação de Acesso

O atributo *accessIdentity* identifica o titular do CA para a aplicação. Neste atributo o campo *authInfo* não deve existir.

O objetivo deste atributo é prover informações sobre o titular do CA, que pode ser usado pelo verificador do CA para autorizar determinadas ações do titular dentro do sistema verificador do CA.

O formato deste atributo é definido abaixo:

```
name      id-aca-accessIdentity
OID       { id-aca 2 }
syntax    SvceAuthInfo
values:   Multiple allowed
```

Identificação de Cobrança

O atributo *chargingIdentity* identifica o titular do CA para o propósito de cobrança. Geralmente o identificador de cobrança será diferente de outros identificadores do titular. Como exemplo, o nome da empresa onde trabalha o titular, será a entidade responsável pelo pagamento de um serviço.

O formato deste atributo é definido abaixo:

```
name      id-aca-chargingIdentity
OID       { id-aca 3 }
syntax    IetfAttrSyntax
values:   One Attribute value only; multiple values within the
          IetfAttrSyntax
```

Grupo

O atributo *group* contém informações sobre o grupo ao qual o titular do CA é membro. O formato deste atributo é definido abaixo:

```
name      id-aca-group
OID       { id-aca 4 }
syntax    IetfAttrSyntax
values:   One Attribute value only; multiple values within the
          IetfAttrSyntax
```

Papel / Função

O atributo *role*, contém informações sobre o papel ou função desempenhado pelo titular do CA. A sintaxe usada para este atributo é a seguinte:

```
   RoleSyntax ::= SEQUENCE {
           roleAuthority   [0] GeneralNames OPTIONAL,
           roleName        [1] GeneralName
}
```

O campo *roleAuthority* pode ser usado para especificar a autoridade do emissor para um determinado papel. Não é obrigatório que este campo represente necessariamente a existência de um emissor responsável pelo atributo. Por exemplo, ele pode ser usado apenas como um separador entre um papel de “administrador” definido pela autoridade “São Paulo”, do “administrador” definido pela autoridade “Rio de Janeiro”.

O campo *roleName* deve existir e deve usar o opção *uniformResourceIdentifier* do campo *GeneralName*. A sintaxe usado para este atributo é a seguinte:

```
name      id-at-role
OID       { id-at 72 }
syntax    RoleSyntax
values:   Multiple allowed
```

Nível de Acesso (*clearance*)

O atributo *clearance* contém informações relativas ao nível de acesso do titular do CA. O campo *policyId* é usado para identificar a política de segurança a qual o nível de acesso está relacionado. Os níveis de acesso pré-definidos são: sem definição, irrestrito, restrito, confidencial, secreto e altamente confidencial.

Uma organização pode criar a sua própria política de segurança, entretanto as posições de 0 a 5 do *BIT STR*ING são reservadas para os níveis de acesso pré-definidos. Se estiver presente, o campo *SecurityCategory* provê informações adicionais de autorização. A sintaxe usada para este atributo é a seguinte:

```
Clearance  ::=  SEQUENCE {
     policyId  [0] OBJECT IDENTIFIER,
     classList [1] ClassList DEFAULT {unclassified},
     securityCategories
               [2] SET OF SecurityCategory OPTIONAL
}

ClassList  ::=  BIT STRING {
     unmarked       (0),
     unclassified   (1),
     restricted     (2)
     confidential   (3),
     secret         (4),
     topSecret      (5)
}

SecurityCategory ::= SEQUENCE {
     type      [0]  IMPLICIT OBJECT IDENTIFIER,
     value     [1]  ANY DEFINED BY type
}

-- This is the same as the original syntax which was defined
-- using the MACRO construct, as follows:
-- SecurityCategory ::= SEQUENCE {
--      type      [0]  IMPLICIT SECURITY-CATEGORY,
--      value     [1]  ANY DEFINED BY type
-- }
--
-- SECURITY-CATEGORY MACRO  ::=
-- BEGIN
-- TYPE NOTATION ::= type | empty
-- VALUE NOTATION ::= value (VALUE OBJECT IDENTIFIER)
-- END
name      { id-at-clearance }
OID       { joint-iso-ccitt(2) ds(5) module(1)
            selected-attribute-types(5) clearance (55) }
syntax    Clearance - imported from [X.501-1993]
values    Multiple allowed
```