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

Jonathan Gehard Kohler

# ANÁLISE DE POLÍTICAS NA INTEGRAÇÃO DE INFRAESTRUTURAS DE CHAVES PÚBLICAS

Florianópolis
2011

Jonathan Gehard Kohler

# ANÁLISE DE POLÍTICAS NA INTEGRAÇÃO DE INFRAESTRUTURAS DE CHAVES PÚBLICAS

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina para a obtenção do grau de mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis
2011

Catalogação na fonte pela Biblioteca Universitária
da
Universidade Federal de Santa Catarina

K79a Kohler, Jonathan Gehard
Análise de políticas na integração de infraestruturas de chaves públicas [dissertação] / Jonathan Gehard Kohler ; orientador, Ricardo Felipe Custódio. - Florianópolis, SC, 2010.
1 v.: il., grafs., tabs.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Ciência da Computação.

Inclui referências

1. Ciência da computação. 2. Certificação digital. 3. Infraestrutura de Chaves Públicas. 4. Interoperabilidade. I. Custódio, Ricardo Felipe. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. III. Título.

CDU 681

Jonathan Gehard Kohler

**ANÁLISE DE POLÍTICAS NA INTEGRAÇÃO DE INFRAESTRUTURAS DE CHAVES PÚBLICAS**

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

Florianópolis, 03 de Março de 2011

---

Prof. Mario Antonio Ribeiro Dantas, Dr.
Coordenador do Curso

**Banca Examinadora:**

---

Prof. Ricardo Felipe Custódio, Dr.
Orientador
Universidade Federal de Santa Catarina

---

Profa. Noemi de La Rocque Rodriguez, Dra.
Pontifícia Universidade Católica do Rio de Janeiro

---

Prof. Olinto José Varela Furtado, Dr.
Universidade Federal de Santa Catarina

---

Renato da Silveira Martini, Dr.
Instituto Nacional de Tecnologia da Informação

---

Prof. Roberto Willrich, Dr.
Universidade Federal de Santa Catarina

À minha família,
pela extraordinária dedicação e apoio.

## AGRADECIMENTOS

Aos meus pais, meu porto seguro, Atanásio e Sueli por toda a atenção e extraordinária dedicação em me auxiliar em minha caminhada da melhor forma possível, nunca faltando com paciência e carinho. Também agradeço aos ensinamentos recebidos, que carregarei por toda minha vida.

Ao orientador desta dissertação, professor Ricardo Felipe Custódio, pela oportunidade e confiança depositada em mim para realizar este trabalho. Também agradeço pelos conhecimentos compartilhados, pela paciência em me auxiliar a escrever este trabalho, e principalmente pelos conselhos.

À minha amada namorada, Camila, por sua confiança, força, amor e sua sinceridade desconcertante. Agradeço também pela paciência nos momentos em que não pude estar ao seu lado, e a beleza que trouxe à minha vida.

Aos colegas do LabSEC, Anderson e César, pelo auxílio na realização dos testes descritos neste trabalho, bem como pelas inestimáveis trocas de experiência. Também foram a minha primeira experiência de docência, em que pude repassar parte do conhecido adquirido ao longo de 5 anos no LabSEC.

À "velha geração" do LabSEC, Felipe, Juliano, Nelson, Thiago, Martín, Armindo, Jeandré, Marcelo, Cristian, Lucas e Leonardo, pelas inúmeras conversas, discussões e opiniões trocadas. Também agradeço à paciência dispendida para me ensinar e auxiliar no início de minha carreira na área de segurança. Não posso deixar de agradecer também a "nova geração" do LabSEC, a qual seria impossível de enumerar todos os nomes aqui, pelo apoio e auxílios prestados em todos os momentos. Agradeço também pelas festas e alegrias compartilhadas.

Ao professor Ricardo Moraes, pelas considerações e sugestões feitas a este trabalho, que contribuiu muito para a qualidade deste trabalho.

À Banca examinadora, por deixar outros compromissos de lado e poder fazer-se presente na apresentação deste trabalho, bem como pelas considerações, perguntas e sugestões

À Rede Nacional de Ensino e Pesquisa (RNP), principalmente os integrantes do projeto Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEDU), pelas experiências e ensinamentos trocados. Além

da RNP, agradeço ao Instituto Nacional de Tecnologia (ITI) e Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ), que possibilitaram me dedicar exclusivamente as atividades de pesquisa.

*"Quando você tem a possibilidade de lutar, você tem a fé, a esperança; ai depende de voce realmente lutar, trabalhar e acreditar que você pode, e ir até o final."*
*(Ayrton Senna, em entrevista após vencer o GP do Brasil em 1991)*

**RESUMO**

Durante as últimas décadas, houve um aumento no número de Infraestruturas de Chaves Públicas. Consequentemente surgiu a necessidade de validar assinaturas digitais independentemente do domínio em que elas foram realizadas. Esta demanda pode ser suprida através da integração de ICPs. Acredita-se que no futuro, ICPs serão imergidas nos mais diversos dispositivos computacionais, e estes necessitarão associar-se para realizar comunicações seguras. Os atuais estudos sobre a gestão de algoritmos e políticas na integração de ICPs, não consideram o cenário de integração de vários dispositivos, objetivo principal desta dissertação. Análises foram feitas sobre os atuais métodos de integração, e testes foram realizados para encontrar as dificuldades de implementação intrínsecas a esses. Diversas lacunas não tratadas na literatura foram encontradas, abrangendo desde a montagem do caminho de certificação até a manutenção da validade de documentos após a dissolução dos domínios. Soluções foram propostas após a análise destas lacunas. Com relação ao gerenciamento dos aspectos políticos, a principal dificuldade encontrada foi a correta realização do mapeamento de políticas de forma totalmente automatizada. Também foram realizadas testes com a integração de domínios com diferentes algoritmos criptográficos. Nesta abordagem, o maior entrave foi a diversidade de padronizações existentes, cada qual sugerindo um conjunto de algoritmos diferentes. Ao final do trabalho, foi realizado um estudo de caso, considerando a integração da ICP-Brasil com outras ICPs, e aplicando as sugestões realizadas anteriormente. Demonstrou-se que as considerações feitas para ambientes de integração de dispositivos em massa, podem ser aplicadas na integração de ICPs organizacionais.

**Palavras-chave**: X.509, Infraestrutura de Chaves Públicas, ICPs Multi-domínio, Relações de Confiança entre ICPs, Políticas de Certificação, Interoperabilidade de ICPs.

**ABSTRACT**

Over the last decades, there was a raise in the number of PKIs. With the expansion, the digital signatures performed into a domain needed to be valid into other domains. This demand can be supplied with the PKI's integration. Is is believed that in the future, PKI will be immersed in various computer devices, and these will need to join each other to perform secure communications. Although there are other studies on the algorithms and policies management in the integration of PKIs, they do not consider the scenario of multiple devices integration, the main purpose of this research. Analyses were made about the current integration methods, apart from simulations to find inherent difficulties on this methods. Several gaps not addressed in the literature were found, ranging from the construction of the certification path to the maintain the validity of documents after the dissolution of the domains. These weaknesses were analyzed and solutions were proposed. With regard to the political management aspects, the main difficult in this research is the correct fully automated policy mapping. Also in this paper, simulations were carried out with the integration of domains with different cryptographic algorithms. In this approach, the biggest obstacle was the diversity of existing standardization, each suggesting a different set of algorithms. At the end, was performed a case study, considering the integration of ICP-Brazil with other PKIs, and applying the suggestions made previously. The case study demonstrates that the previous assumptions made for massive devices integration environments may be applied in the integration of organizational PKIs.

**Keywords**: X.509, Public Key Infrastructure, Multi-Domain PKI, Trust Relationship across PKIs, Certificate Policies, PKI interoperability.

## LISTA DE FIGURAS

## LISTA DE TABELAS

**LISTA DE ABREVIATURAS E SIGLAS**

AC - Autoridade Certificadora
ACT - Autoridade de Carimbo do Tempo
AIA - Authority Information Access
AMCT - Autoridade Múltipla de Carimbo do Tempo
CAdES - CMS Advanced Electronic Signature
CMS - Cryptographic Message Syntax
DN - Domain Name
DPC - Declaração de Práticas de Certificação
ECC - Elliptic curve cryptography
ETSI - European Telecommunications Standards Institute
GWCA - Gateway Certification Authority
HSM - Hardware Security Module
IANA - Internet Assigned Numbers Authority
ICP - Infraestrutura de Chaves Públicas
IFC - Integer factorization cryptography
JCA - Java Cryptography Architecture
LCC - Lista de Certificados Confiáveis
LCR - Lista de Certificados Revogados
NFS - Number Field Steve
NIST - National Institute of Standards and Technology
NSS - Mozilla Network Security Services
OCSP - Online Certificate Status Protocol
OID - Identificador de Objeto
PAdES - PDF Advanced Electronic Signature
PC - Política de Certificado
RFC - Request for Comment
SECG - Standards for Efficient Cryptography Group
SDSI - Simple Distributed Security Infrastructure
SPKI - Simple Public Key Infraestructure
SVCP - Server-Based Certificate Validation Protocol
URL - Uniform Resource Locator
XAdES - XML Advanced Electronic Signature
XML - Extensible Markup Language
XMLDsig - XML Digital Signature

**SUMÁRIO**

# 1 INTRODUÇÃO

Chaves criptográficas assimétricas têm sido usadas para a identificação de pessoas e equipamentos desde que foram propostas por Diffie e Hellmann em 1976. A chave privada é mantida sob o controle da entidade identificada e a chave pública pode ser divulgada através de certificados digitais. Os certificados digitais são emitidos por autoridades certificadoras que fazem parte de uma infraestrutura de chaves públicas (ICP). A autoridade certificadora tem a responsabilidade de verificar os dados da entidade e garantir que a chave privada foi gerada e é mantida sob custódia da entidade. Com isso, a entidade não pode negar o uso de sua chave privada, e esta pode ser usada para assinar mensagens eletrônicas ou para fins de autenticação.

Normalmente, cada entidade possui um certificado digital para sua identificação. Esse certificado tem uma duração pré-determinada, estabelecida pela autoridade certificadora no momento da sua emissão. Se por qualquer motivo, os dados de identificação contidos no certificado deixarem de ser válidos, a autoridade certificadora revoga o certificado. As autoridades certificadoras comunicam os usuários da situação de revogação de um certificado através de listas de certificados revogados[3]. Podem também usar protocolos de verificação online, tais como o OCSP [4], SVCP [5] e outros.

A gestão do ciclo de vida de certificados digitais é feita por uma infraestrutura de chaves públicas. Uma ICP é formada por uma série de elementos (serviços), cada um deles responsável por algum aspecto relacionado ao ciclo de vida do certificado digital. Tradicionalmente, desde que foram propostas por Konfelder [6], RFC5280 [3] e X.509 [7] , as ICPs são criadas para gerir certificados digitais dentro de um domínio fechado. É praxe, por exemplo, criar-se ICPs para um país, um bloco econômico ou uma empresa.

Dentro de um domínio, cada usuário necessita apenas confiar nas suas âncoras de confiança. Na grande maioria das implementações práticas de ICPs, as âncoras são certificados digitais autoassinados que representam autoridades certificadoras raízes. Ainda dentro de um domínio, é relativamente tranquilo estabelecer-se políticas e práticas de comum acordo entre todos os participantes para manter a confiança tanto nas assinaturas digitais quanto em processos de autenticação. Por razões práticas, mesmo as âncoras tem um tempo de vida limitada. Para manter o funcionamento de todos os serviços e aplicações dentro do domínio, novas âncoras de confiança são criadas ao longo do tempo, mas todas elas, de alguma forma, são propagadas a todos os usuários, garantindo a integração dos serviços e reconhecimento das assinaturas digitais por todos.

Acontece que, ICPs têm sido criadas em vários contextos, e as as-

sinaturas de mensagens realizadas dentro de um domínio, passaram a necessitar serem válidas em outros domínios. Isso pode ser feito a partir da integração de ICPs. Vários mecanismos foram propostos na literatura para permitir esta integração. Segundo Housley [**?**], os mais conhecidos são as listas de certificados confiáveis, certificação cruzada e pontes.

No entanto, apesar da previsão de integração de ICPS em diversos mecanismos, vários problemas dificultam em demasia sua implementação. Em especial, o mapeamento de políticas entre ICPs não é uma tarefa trivial, como será exposto ao longo deste trabalho.

Nesta pesquisa, e trabalhando com ICPs em vários contextos ao longo de cinco anos, tais como ICPs para universidades e centros de pesquisa [9], vislumbrou-se que ICPs poderiam ser criadas em contextos mais limitados, tal como em um equipamento. No LabSEC, onde este trabalho de dissertação foi desenvolvido, foi projetado um dispositivo criptográfico, denominado em Inglês por Hardware Security Module (HSM), para a gestão de chaves privadas de autoridades certificadoras. Durante o projeto deste equipamento, deparou-se com vários desafios para gerir de forma plena e confiável as chaves privadas sob a sua guarda. E concluímos que a melhor forma de contornar os problemas advindos desses desafios seria implementar uma ICP dentro do equipamento. Assim, o equipamento teria uma autoridade certificadora raiz, e outras ACs intermediárias e finais, as quais emitiriam certificados digitais a todos os *principals* internos do dispositivo. Esta necessidade também foi percebida em outros projetos do LabSEC que necessitavam efetuar trocas seguras de mensagens.

Um problema surgiu dessa estratégia. Como integrar dois dispositivos criptográficos, cada um deles com sua própria ICP? Será que aquelas técnicas de integração, propostas para grandes domínios, poderiam ser utilizadas nesse novo cenário? Este novo cenário pode trazer novos desafios para realizar integrações?

Além disso, poderíamos imaginar que haveria um grande número de dispositivos cada um com sua ICP para serem integrados. Pergunta-se, num cenário de dezenas, talvez centenas de dispositivos, as técnicas de integração conhecidas seriam adequadas?

Várias razões nos impelem a acreditar, que as entidades, pelo menos aquelas com algum grau de computação (com sistema operacional, memória e CPU), deveriam cada uma delas ter uma ou mais ICPs. Como são um número enorme de entidades nesse cenário, acredita-se que deve-se repensar as técnicas e modelos de integração de ICPs de forma a serem efetivas e alcançarem o seu objetivo. Neste trabalho, estuda-se, por fim, esses novos cenários e avalia-se as técnicas de integração, além de sugerir modificações e melhoras que podem sobrepujar os problemas que surgem desse novo cenário.

## 1.1 OBJETIVOS

### 1.1.1 Objetivo Geral

O principal objetivo deste trabalho é analisar e propor mecanismos que permitam a integração de infraestruturas de chaves públicas considerando domínios de certificação embarcados em dispositivos. Em particular, está-se interessado nas políticas de certificação de cada infraestrutura membro e seu comportamento a longo prazo nas assinaturas digitais.

### 1.1.2 Objetivos Específicos

Os objetivos específicos deste trabalho são:

- Descrever os mecanismos de integração consolidados na literatura;
- Levantar as propriedades de uma infraestrutura de chaves públicas que devem ser preservadas em longo prazo e compartilhadas entre as infraestruturas integradas;
- Mostrar como é feita a gestão das âncoras de confiança das infraestruturas de chaves públicas na integração de diferentes domínios e propostas que visem melhorar essa gestão;
- Criar um ambiente para realizar experimentos de integração de infraestruturas de chaves públicas;
- Realizar simulações de integração de infraestruturas de chaves públicas e descrever todos os efeitos sobre as mensagens assinadas e os protocolos de autenticação que utilizam as chaves certificadas;
- Discorrer sobre a preservação em longo prazo de assinaturas digitais à luz da integração de infraestruturas de chaves públicas;
- Apresentar propostas que permitam mitigar os efeitos malévolos decorrentes do processo de integração de infraestrutura de chaves públicas
- Justificar e defender a proposta de que existirão no futuro incontáveis infraestruturas de chaves públicas, cada qual necessária para gerir de forma confiável o ciclo de vida de chaves criptográficas utilizadas em sistemas de informação e comunicação;
- Descrever os processos de mapeamento de políticas de certificação digital;
- Apresentar um estudo de caso de integração entre infraestrutura de chaves públicas governamentais;
- Avaliar o efeito em longo prazo, dos algoritmos criptográficos em relação a integração de infraestrutura de chaves públicas.

## 1.2 JUSTIFICATIVA

É consenso entre os estudiosos de aplicações de criptografia que todos os sistemas serão no futuro identificados por uma chave pública. E estas serão imersas dentro de certificados digitais para garantir sua autenticidade e integridade. Adicionalmente, os sistemas serão agrupados em domínios, cada um desses com suas respectivas âncoras de confiança. Tais âncoras são necessárias para validar as chaves públicas e permitir a assinatura digital de mensagens e realizar processos de autenticação dos seus membros intra-domínio.

Acontece que, frequentemente, um membro de um domínio precisa trocar mensagens ou se autenticar perante um membro de outro domínio. Na prática, é necessário que os domínios sejam integrados de alguma forma para que isso seja possível. Isso, de fato, já é preocupação de praticamente todos os modelos de certificação digital existentes. Há mecanismos para realizar tais integrações, entre os mais conhecidos estão a certificação cruzada e a certificação em ponte. No entanto, na prática, pouco se tem feito em relação à integração. Sabe-se que foram realizadas algumas iniciativas de integração de infraestruturas de chaves públicas utilizando pontes, como por exemplo a ICP Norte-Americana *The US Federal PKI*, que criou a ponte *Federal Bridge Certification Authority* [10] para conectar os diversos órgãos governamentais norte-americanos, a comissão Européia criou uma ponte para integrar os serviços da administração pública de seus países membros, a *European Bridge CA* [11]. Temos também como exemplo o governo Japonês, em que adotou o modelo de ponte para unificar as suas ICPs governamentais pré-existentes [12]. Contudo, não se tem conhecimento da existência de um estudo que leva em consideração a possibilidade de que no futuro todos os sistemas sejam identificados por certificados digitais. Isso implica na possibilidade de existirem inúmeras ICPs.

Acredita-se que um trabalho acadêmico sobre os mecanismos de integração existentes e, se esses poderiam ser utilizados na integração em larga escala de infraestruturas de chaves públicas, seria muito útil e poderia esclarecer a viabilidade da certificação digital em massa. Se for possível, no futuro teremos maior segurança nas transações eletrônicas entre os mais diversos tipos de sistemas.

## 1.3 MOTIVAÇÃO

O Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina, local onde este trabalho de mestrado foi realizado, tem desenvolvido inúmeros trabalhos científicos e tecnológicos na área de certificação digital e suas aplicações. Um dos projetos do LabSEC é o desenvolvimento de soluções que permitam a independência tecnológica da infraestrutura de chaves públicas brasileira. O LabSEC foi uma das entidades responsável pelo projeto da nova plataforma crip-

tográfica da ICP-Brasil.

Uma das grandes preocupações da ICP-Brasil e do LabSEC é em relação a integração da ICP-Brasil com ICPs de outros países. Já houve contato, por exemplo, de Portugal solicitando ao Brasil um estudo que viabilizasse a integração entre as infraestruturas de chaves públicas brasileira e portuguesa. Após alguns estudos preliminares, foi concluído que os mecanismos descritos na literatura e também das experiências realizadas por países e blocos econômicos não foram conclusivos e apresentaram vários desafios que precisam ser resolvidos para viabilizar com sucesso essas integrações.

Além disso, os desenvolvimentos de soluções de certificação digital feitos dentro do LabSEC mostraram que o uso de infraestruturas internas aos sistemas seria uma solução interessante para a gestão de confiança em processos internos desses sistemas. Surge então, a oportunidade de se estudar como poderia ser feito a integração das mais diversas infraestruturas, sejam elas governamentais ou simplesmente infraestruturas internas de sistemas computacionais.

Realizaram-se alguns experimentos no LabSEC sobre o processo de integração e após um levantamento prévio na literatura especializada, conclui-se que um trabalho de mestrado neste assunto seria oportuno. Isso motivou a proposta deste trabalho de dissertação.

## 1.4 DELIMITAÇÃO DO TRABALHO

Existem diversos aspectos a serem considerados na integração de ICPs, e este trabalho limita-se às questões relacionadas com autenticação de entidades, assinaturas de documentos eletrônicos, e certificados de carimbo de tempo. Aspectos de compatibilidade de implementação de aplicativos, como diferenças de codificações entre os sistemas a serem integrados, não foram considerado. Também não serão tratados os aspectos político-administrativos relativos à criação, gestão e manutenção de pontos de confiança, ou de autoridades de confiança.

Para haver a integração entre dispositivos, inicialmente é necessário haver um protocolo para identificar que existem dispositivos disponíveis para realizar a comunicação. Estes aspectos, bem como os aspectos técnicos sobre a forma de comunicação entre os dispositivos a serem integrados não serão tratados neste trabalho, o qual apenas assume que existe um conjunto de dispositivos que necessitam realizar uma comunicação de forma segura, através do uso de suas ICPs internas.

Existem outros modelos de certificação, tais como como o PGP [13], SPKI [14, 15], entre outros, entretanto, estes não serão tratados neste trabalho, que se restringe ao padrão X.509[7].

## 1.5 METODOLOGIA

O início deste trabalho se deu a partir da coleta, leitura, interpretação e análise das principais normas e padrões disponíveis na literatura que se referissem a integração de domínios de ICPs, interoperabilidade em ICP e gerência de âncoras de confiança em múltiplos domínios.

Após isso foram estudadas as principais ICPs que utilizavam alguns dos mecanismos encontrados na pesquisa anterior. Foram pesquisadas e analisadas as infraestruturas: *The US Federal PKI*, *European Bridge CA*, *Japanese Government PKI* e *CertiPath Bridge*.

Os resultados destes estudos permitiram gerar inúmeros mecanismos e formas diferentes de realizar a integração entre duas ICPs. Foram criados diversas ICPs com as mais variadas topologias possíveis, representando as possíveis ICPs internas de dispositivos.

As integrações foram simuladas com a ajuda de algumas bibliotecas criptográficas, como OpenSSL [16], BouncyCastle [17], Java Cryptography Architecture [18](JCA), Mozilla Network Security Services [19](NSS) e Microsoft Cryptographic API: Next Generation [20](CryptoAPI). Os mecanismos que não foram possíveis de serem simulados, seja por limitações teóricas ou tecnológicas, não foram considerados como soluções para os resultados.

Após os primeiros resultados serem produzidos, foi realizado um estudo de caso, aplicando os conhecimentos adquiridos para tentar localizar limitações práticas, e se necessário propor correções e melhorias. O estudo de caso foi constituído pela criação de um clone[1] da Infraestrutura de Chaves Pública Brasileira (ICP-Brasil). Sabendo-se do interesse manifestado por Portugal, foi criado um clone da ICP portuguesa, e foram realizadas simulações integrando estas duas ICPs. Através destas simulações foram encontradas algumas limitações na integração destas ICPs, e foram propostas modificações e melhorias, justificando estas através de normas e trabalhos da literatura.

Posteriormente foram feitas novas simulações, agora para integração da ICP-Brasil com os países integrantes do bloco econômico Mercado Comum do Sul (Mercosul), atualmente o mais influente na economia brasileira.

Durante as simulações foram analisados diversos aspectos, tais como a autenticação de entidades entre os domínios, a montagem e validação do caminho de certificação, a validação de assinaturas digitais, a manutenção da validade de assinaturas digitais por longo prazo, os efeitos causados pela desagregação de uma das ICPs, a integração de diferentes algoritmos criptográficos, entre outros aspectos.

Os resultados encontrados a partir destes estudos, análises e simulações, permitiram concluir que após a integração das ICPs, certos aspectos analisados poderiam ser comprometidos, dependendo da forma como as ICPs foram criadas e implementadas.

[1] Os pares de chaves privada e pública eram diferentes.

Por fim, foram estudadas formas de suprir estas carências. Algumas destas necessitavam de pré-condições, que deveriam ser satisfeitas pelas ICPs, outras apresentavam diversas possíveis soluções. Por fim, foram utilizadas ICPs simuladas anteriormente para realizar testes e verificar a viabilidade das soluções encontradas.

## 1.6 TRABALHOS RELACIONADOS

Após a publicação do artigo científico de Diffie e Hellman [21] propondo a criptografia de chaves públicas em 1976, vislumbrou-se a possibilidade de realizar assinatura digital e autenticação em sistemas eletrônicos. Em 1978, Konfelder [6] propôs o uso de certificados digitais para facilitar a promoção das chaves públicas associadas aos seus titulares. Em meados da década de 1980, a tecnologia evoluiu de tal forma que organismos internacionais já estavam propondo normas para a gestão do ciclo de vida de certificados e chaves criptográficas. Já nessa época havia a idéia de se realizar a integração de domínios de certificação digital.

Vários países e empresas, diante das vantagens de que poderiam usufruir, procuraram criar suas infraestruturas de chaves públicas e surgiram algumas empresas prestadoras de serviços de certificação digital. A maior das aplicações, e isso ocorre até hoje, foi a viabilização do internet banking através de túneis seguros de comunicação, construídos usando o protocolo SSL.

Vislumbra-se inúmeras outras aplicações para a certificação digital. Entretanto, no início deste século, surgiram muitos problemas no seu uso. As pesquisas, por exemplo em termos de artigos publicados começaram a ficar escassas. Alguns pesquisadores defendiam a idéia de que os modelos de certificação existentes estavam inadequados e que era necessário outra tecnologia para prover os serviços de uma infraestrutura de chaves públicas. Outros, como [22], [23], [24] e [25], defendiam que os modelos de certificação não eram adequados para prover os serviços, e necessitavam de várias modificações e adaptações.

Infraestrutura de chaves públicas simples, em inglês Simple Public Key Infraestructure (SPKI) [14, 15] foi concebida para resolver alguns dos conhecidos problemas da tradicional infraestrutura de chaves públicas X.509. O SPKI define um formato de certificado de autorização, o qual permite associar a chave pública privilégios, direitos e atributos. Em SPKI tanto a chave pública quanto autorizações podiam ser associadas às entidades. Além disso, diferentemente do X.509, era permitida a delegação de autorização a outras chaves públicas.

Em 1996, SPKI foi unida com a Infraestrutura de Segurança Distribuída Simples, em inglês Simple Distributed Security Infrastructure (SDSI) proposta por Ronald L. Rivest e Butler Lampson em [26] criando a SPKI/SDSI. Nessa nova arquitetura, era permitido também criar nomes para entidades e a delegação de direitos e atributos de uma entidade para outra.

Apesar de ter conceitos mais avançados de gestão de chaves públicas, direitos, atributos, com a adição da delegação, ou seja, um determinado direito poderia ser delegado a outra entidade, a SPKI/SDSI não foi adotada comercialmente. O principal motivo, acredita-se, é a dificuldade de rastreamento da delegação e a responsabilização dos titulares dos certificados. Essa arquitetura tem sido somente usada em domínios fechados, em especial, em projetos de interesse acadêmico, como o projeto "Cadeias de Confiança"[27].

Em relação a integração de ICPs, os principais mecanismos existentes mais conhecidos são três: uso de certificação cruzada, bridges e lista de certificados confiáveis. Na literatura podem ser encontradas algumas abordagens que tentam simplificar alguns aspectos, como por exemplo o trabalho de Li[28], que dentre outros aspectos, tenta diminuir os custos da integração da autenticação intra-empresarial, através da criação de Autoridades Certificadoras Virtuais. Este trabalho faz a integração através da criação de um novo ponto de confiança temporário (virtual), em que o controle da chave privada é realizado através de compartilhamento de segredo. O foco principal deste trabalho é a comunicação entre empresas, e necessita de um acordo efetuado por todos os integrantes no momento da criação da AC.

Também é importante citar o trabalho de Guo[29], que cria um novo conceito de autoridade certificadora, chamado de *Gateway CA (GWCA)*. Neste trabalho, diversas GWCAs estão conectadas através de uma configuração em anel, e estas compartilham a mesma chave pública, porém possuem diferentes chaves privadas. A proposta ainda define que estas GWCAs precisam ser o ponto de confiança de todos os usuários participantes. Esta característica torna esta abordagem impraticável para integrar ICPs em larga escala, pois cada domínio geralmente já possui o seu ponto de confiança.

Há também o trabalho de Bickenbach et al[30], que define diversos aspectos técnicos que devem ser seguidos para aumentar a interoperabilidade entre aplicações, no entanto, este apenas considera os aspectos de interoperabilidade intra-domínio, sendo omisso em alguns casos necessários para integrar diversas ICPs. A RFC5217 [31] trata dos modelos de integração possíveis, mas não considera os aspectos técnico-práticos necessários.

A figura 1.1 apresenta a relação existente entre este trabalho e os encontrados na literatura. Os trabalhos encontrados apresentam soluções para integração de ICPs considerando a integração de grandes domínios. Este trabalho analisa o mesmo processo de integração de ICPs, porém com um novo foco, a integração de ICPs embarcadas em dispositivos. Foco este que não foi abordado em nenhum dos outros trabalhos encontrados na literatura. A análise dos processos de integração de ICPs sob este novo foco, adiciona diversas características inerentes a ambientes de dispositivos, que se diferenciam em vários aspectos relacionados a integração de ICPs de grande porte. Estas características, e os desafios

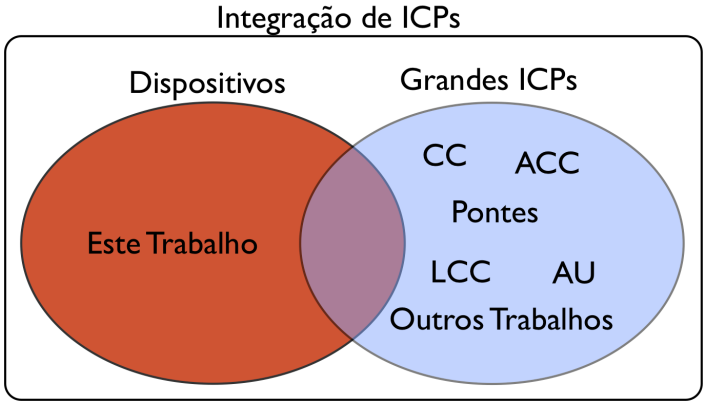


**Figura 1.1:** Ambientação dos trabalhos relacionados

encontrados serão apresentados no decorrer deste trabalho.

## 1.7 ORGANIZAÇÃO DO TRABALHO

O capítulo 2 apresenta uma introdução sobre algoritmos criptográficos, além de fazer um breve relato das propriedades e boas práticas que devem ser consideradas ao gerar uma chave. O capítulo 3 discute os principais fundamentos de ICP necessários para a compreensão deste trabalho, tais como assinatura digital, caminho de certificação, âncoras de confiança, entre outros. Neste capítulo também são explanados os principais elementos de confiança de uma ICP. O capítulo 4 apresenta os principais conceitos relativos ao tratamento de políticas em uma ICP, além de explanar as extensões de certificados digitais utilizadas para incorporar conceitos políticos. O capítulo 5 demonstra algumas alternativas encontradas para realizar a integração de ICPs internas em dispositivos, e como realizar a validação da assinatura digital entre as diferentes ICPs. Este capítulo também apresenta algumas alternativas para a preservação de documentos a longo prazo na integração de ICPs. O capítulo 6 apresenta uma análise sobre o estudo de caso conduzido na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). No capítulo 7 são apresentadas as considerações finais do trabalho, assim como possíveis trabalhos futuros.

# 2 ELEMENTOS CRIPTOGRÁFICOS

## 2.1 INTRODUÇÃO

Durante a geração de um par de chaves, é necessário efetuar a escolhe de algum algoritmo criptográfico, onde alguns pontos importantes devem ser considerados. Primeiramente, deve-se garantir que a chave utilize um algoritmo que supra as necessidades dos aplicativos que farão uso dessa chave. Por exemplo, um determinado sistema, que possui capacidade limitada, pode não conseguir operar com chaves muito longas. Neste caso a escolha do algoritmo errado pode inibir a realização da funcionalidade daquele sistema. Outro ponto importante a ser considerado é o tempo em que a chave vai ser utilizada. Uma chave assimétrica de tamanho pequeno não pode ser utilizada por muito tempo, pois a evolução da capacidade de processamento dos computadores poderá permitir que a chave privada seja derivada da chave pública em pouco tempo. Estes pontos serão discutidos nas próximas seções.

## 2.2 PRINCÍPIOS DAS CHAVES

Recomenda-se que uma chave não seja utilizada para mais de um único propósito [1]. Existem algumas razões para isto:

- O uso da mesma chave para dois processos criptográficos diferentes pode enfraquecer a segurança de um ou de ambos processos.
- Limitar os uso de uma chave, limita os danos que podem ser feitos caso a chave seja comprometida.
- Alguns usos de uma chave, podem interferir em outros usos.

Estes princípios não são válidos nos casos em que um único processo utilizando uma única chave provê vários “serviços”. Por exemplo, uma assinatura digital pode prover irretratabilidade, autenticação e integridade dos dados com apenas uma assinatura [1, p. 44].

## 2.3 ALGORITMOS DAS CHAVES

Algoritmos criptográficos possuem diferentes “forças”, dependendo do algoritmo e do tamanho da chave utilizada [1, p. 61].

A força de um algoritmo para um determinado tamanho de chave (X) é normalmente descrita através do esforço necessário para tentar todas as possíveis chaves de um algoritmo simétrico.

Segundo Barker et al [1, p. 61], dois algoritmos são considerados com forças equivalentes para as chaves de tamanho X e Y quando a quantidade de trabalho necessária para "quebrar os algoritmos" ou determinar as chaves é aproximadamente a mesma, utilizando um dado recurso . Um algoritmo assimétrico que possui uma chave de "Y" bits, e que a força é equivalente a uma chave de "X" bits de um algoritmo simétrico, é dito ter a força de "X" bits, ou, possui "X" bits de segurança. Esta afirmação é expressa pela equação 2.1, onde $f(X)$ = força do algoritmo $X$, e $qt(r, X)$ representa a quantidade de trabalho para quebrar o algoritmo $X$ utilizando um recurso $r$.

$$f(X) \equiv f(Y) \Leftrightarrow qt(r, X) \cong qt(r, y) \tag{2.1}$$

Determinar a força de um algoritmo pode ser uma tarefa não trivial. A evolução da fatoração de algoritmos, ataques a logaritmos discretos, ataques a curvas elípticas e a computação quântica podem afetar a força dos algoritmos no futuro.

A tabela 2.1 apresenta um comparativo entre algoritmos simétricos e assimétricos que possuem a mesma força.

| Bits de segurança | Algoritmo Simétrico | IFC (ex. RSA) | ECC (ex. ECDSA) |
|---|---|---|---|
| 80 | 2TDEA | 1024 | 160-223 |
| 112 | 3TDEA | 2048 | 224-255 |
| 128 | AES-128 | 3072 | 256-383 |
| 192 | AES-192 | 7680 | 384-511 |
| 256 | AES-256 | 15360 | 512+ |

**Tabela 2.1:** Equivalência de força entre algoritmos. Adaptado de Barker et al.[1]

A primeira coluna apresenta o número de bits de segurança que os algoritmos (com os respectivos tamanhos de chaves mencionados) fornecem. Vale ressaltar, que o número de bits de segurança não é necessariamente o mesmo que o tamanho da chave dos algoritmos das outras colunas. Isto ocorre, pois, estes algoritmos possuem ataques que diminuem a força necessária para quebrá-los.

A segunda coluna apresenta os algoritmos simétricos que possuem, no mínimo, o número de bits de segurança igual ao determinado pela primeira coluna. Por exemplo, o algoritmo 2TDEA possui 80 bits de segurança, enquanto que o 3TDEA possui 112 bits de segurança. Os algoritmos 2TDEA e 3TDEA estão descritos em [32], AES está descrito em [33].

A terceira e quarta colunas indicam o tamanho de chave necessária para o algoritmo especificado possuir a quantidade de bits de segurança descrito na primeira coluna da tabela. A terceira coluna considera os algoritmos que são baseados na fatoração de números inteiros – *integer factorization cryptography (IFC)* – sendo o RSA o mais conhecido deles. A quarta coluna considera os algoritmos que são baseados em curvas

elípticas – *Elliptic curve cryptography* (ECC) – sendo o ECDSA o mais conhecido.

Em muitos casos, um mesmo algoritmo de chave pode utilizar várias funções hash diferentes. Segundo Barker et al[1, p. 63], o tamanho de uma função resumo (ou função de *hash*) é determinado pelo algoritmo, ou pelo esquema em que a função resumo é utilizada. Por esta razão, os padrões que definem os algoritmos criptográficos devem especificar o tamanho do *hash* apropriado.

A tabela 2.2, adaptada de [1], apresenta as recomendações de algoritmos e tamanhos de chaves que devem ser utilizadas para aplicações não classificadas do Governo Federal Americano (Federal Government).

A primeira coluna da tabela 2.2 indica o período de tempo estimado em que os dados protegidos pelos algoritmos especificados permanecerão seguros. Esta estimativa foi realizada pelo NIST, e publicada em [1]. A segunda coluna apresenta o número de bits de segurança necessários para cada período. Até o final de 2010 devem ser utilizado no mínimo 80 bits de segurança. Entre 2011 e 2030, um mínimo de 112 bits de segurança, e após 2030, pelo menos 128 bits de segurança. A terceira e quarta colunas indicam os tamanhos mínimos de uma chave para os algoritmos baseados em IFC e curvas elípticas, respectivamente, possuírem a quantidade de bits de segurança indicados na segunda coluna. O principal exemplo de algoritmo baseado em IFC é o RSA, e em curvas elípticas é o ECDSA. A última coluna indica os tamanhos possíveis de hashes da família SHA que podem ser utilizados para os algoritmos especificados nas colunas anteriores para realizar assinaturas digitais.

Embora a tabela 2.2 apresente o algoritmo SHA-1 com 80 bits de segurança, recentemente foi demonstrado que o SHA-1 provê 69 bits de segurança. O uso do SHA-1 não é recomendável para geração de assinaturas digitais em novos sistemas, nestes é fortemente sugerido utilizar algoritmos maiores [1].

Vale ressaltar também, que as únicas curvas elípticas ECDSA recomendadas pelo NIST, através do documento [34] para aumentar a compatibilidade entre as aplicações, são as curvas P-256 e P-384. Se esta recomendação for utilizada, nas segunda e terceira linhas da tabela deve ser utilizado pelo menos a curva P-256, que é a que menor curva recomendada que satisfaz os requisitos de tamanho mínimo da chave. Mais informações sobre estas curvas podem ser encontradas na seção 2.5.

Se uma assinatura digital fosse realizada em 2010, e esta necessitar se manter segura por 10 dez anos (até 2020), é sugerido que se utilize uma chave RSA de no mínimo 2048 bits. Se uma chave de tamanho menor for utilizada (por exemplo 1024), esta assinatura pode não oferecer proteção suficiente entre os anos de 2011 e 2020. Em adição ao tamanho da chave, faz-se necessário utilizar alguns dos algoritmos descritos na linha “Até 2030”.

Quando uma função resumo (*hash*) for utilizada com um algoritmo de assinatura utilizando uma combinação de forças diferentes, a

| Algorithm security lifetime | Bits de segurança | IFC (ex. RSA) | ECC (ex. ECDSA) | *HASH* para algoritmos de Assinatura |
|---|---|---|---|---|
| Até 2010 | 80 | 1024 | 160 | SHA1, SHA-224, SHA-256, SHA-384, SHA-512 |
| Até 2030 | 112 | 2048 | 224 | SHA-224, SHA-256, SHA-384, SHA-512 |
| Depois 2030 | 128 | 3072 | 256 | SHA-256, SHA-384, SHA-512 |
| | 192 | 7680 | 384 | SHA-384, SHA-512 |
| | 256 | 15360 | 512 | SHA-512 |

**Tabela 2.2:** Tamanhos mínimos de chaves e *hashes* recomendados pelo NIST para assinaturas digitais, considerando a validade dos algoritmos. Adaptado de [1, p. 63-64]

força da assinatura digital é determinada pelo mais fraco dos algoritmos utilizados [1]. Por exemplo, se o algoritmo SHA-384 (que provê 192 bits de segurança) for utilizado com o algoritmo RSA com uma chave de 2048 (112 bits de segurança), a força da assinatura será de 112 bits de segurança. Outro exemplo, se for necessário que uma assinatura se mantenha segura por 25 anos, é necessário utilizar uma chave RSA com tamanho mínimo de 3072 bits, e função resumo SHA-256. Qualquer combinação utilizando algoritmos mais fracos não irá fornecer a proteção necessária para a assinatura digital.

Quando um algoritmo ou chave não provê mais a proteção necessária para uma determinada informação (algoritmo quebrado, chave roubada etc), qualquer informação protegida pelo algoritmo ou pela chave passa a ser considerada exposta (por exemplo, deixa de ser confidencial, ou a integridade não pode ser verificada) [1, p. 68]. Embora esta informação possa ser protegida novamente (utilizando novos algoritmos) utilizando-se uma cópia da informação armazenada em uma fonte confiável, deve-se assumir que o conteúdo cifrado podem ter sido coletado por um atacante, e este pode decifrar o conteúdo da informação cifrada utilizando ataques sobre o primeiro algoritmo ou chave. Neste caso, mesmo que a informação foi re-protegida, o atacante teve acesso ao conteúdo dela.

| Data de geração da assinatura | Algoritmos e Tamanho das Chaves | Algoritmos de *HASH* |
|---|---|---|
| Até 31/12/2010 | RSA(2048, 3072 ou 4096 bits) | SHA-1 |
| | | SHA-256 |
| | ECDSA (P-256) | SHA-256 |
| | ECDSA (P-384) | SHA-384 |
| Depois 31/12/2010 | RSA(2048, 3072 ou 4096 bits) | SHA-256 |
| | ECDSA (P-256) | SHA-256 |
| | ECDSA (P-384) | SHA-384 |

**Tabela 2.3:** Tamanhos de chaves e *hashes* recomendados pelo NIST para assinaturas digitais para ACs. Adaptado de Barker et al[2, p. 22]

Portanto, ao considerar-se a vida útil de uma informação, deve-se ter cuidado para não escolher algoritmos (e tamanhos de chaves) cuja validade seja menor que o prazo de vida útil da informação.

A escolha do algoritmo criptográfico ideal, além de considerar a proteção necessária da informação, deve considerar os custos decorrentes da transição futura (se necessário) para novos algoritmos. A escolha do algoritmo mais forte nem sempre é a melhor escolha, pois a escolha de algoritmos ou chaves de tamanhos desnecessariamente grande podem afetar o desempenho de determinados dispositivos. Um ambiente onde isto pode ser observado é em dispositivos móveis, em que um algoritmo pode se tornar inaceitavelmente lento se executado com uma chave muito grande.

O NIST faz a recomendação de determinados algoritmos e tamanhos de chaves para serem utilizados por ACs e servidores OCSP [2]. A tabela 2.3 apresenta um resumo destas recomendações.

Na tabela 2.3, a primeira coluna apresenta a data de geração da assinatura, as segunda e terceira colunas demonstram o algoritmo de chave (juntamente com o tamanho da chave) e o algoritmo de hash que recomenda-se ser utilizado no período designado pela primeira coluna. Assinaturas geradas até o final de 2010 podem utilizar chaves RSA de 2048, 3072 ou 4096 bits com os algoritmos SHA-1 ou SHA-256. As chaves geradas até o final de 2010 que utilizarem a curva P-256, recomenda-se que utilizem o algoritmo de *hash* SHA-256, enquanto que para a P-384, recomenda-se o SHA-384. A partir de 31 de dezembro de 2010, não é mais recomendável utilizar o algoritmo SHA-1.

## 2.4 PERÍODO CRIPTOGRÁFICO(CRYPTOPERIOD)

Geralmente as chaves públicas de um indivíduo são distribuídas através de certificados digitais, porém, o período criptográfico de um par

de chaves não necessariamente é o mesmo que o período de validade de um certificado [1].

O Período Criptográfico é o intervalo de tempo durante o qual uma chave está autorizada a ser utilizada por entidades legítimas, ou o tempo que as chaves ficarão em vigor para serem utilizadas por um determinado sistema[1, p. 46]. Um Período Criptográfico adequadamente definido limita:

- A quantidade de informações disponíveis para a criptoanálise das informações protegidas por uma certa chave;
- A quantidade de informações expostas caso ocorra o comprometimento de apenas uma chave;
- O uso de um determinado algoritmo até o seu período de validade estimado;
- O tempo disponível para tentativas de penetração física e lógica nos mecanismos de proteção de tentativa de usos não autorizados da chave;
- O período que uma informação pode ser comprometida pela exposição inadvertida de material criptográfico à entidades não autorizadas;
- O tempo disponível para ataques intensivos de criptoanálise (nas aplicações que não necessita proteção da chave a longo prazo).

O período criptográfico depende, principalmente, do propósito para o qual a chave será utilizada. Os usos podem ser classificados em três categorias: autenticação, transporte de chaves e assinatura digital.

O período criptográfico de uma chave privada utilizada para o transporte de chaves pode ser maior que o período criptográfico associado à chave pública. A chave pública é utilizada por um período fixo de tempo para cifrar materiais criptográficos. Esta validade pode estar indicada em um certificado digital, através da data de expiração. Por outro lado, a chave privada precisa ser retida até o término da necessidade de decifrar o material criptográfico cifrado com a chave pública do certificado. Por exemplo, uma aplicação utiliza certificação digital para fazer o transporte de chaves e após o certificado expirado é necessário acesso ao material criptográfico cifrado. Esta vai precisar da chave privada para decifrar o material criptográfico, mesmo com o certificado já expirado.

Uma chave privada utilizada para autenticação possui geralmente o mesmo período criptográfico que a sua chave pública associada. Isto deve-se ao fato de que quando uma chave privada não é mais utilizada para assinar um desafio (parte do protocolo de autenticação que atesta a autenticidade do usuário), a chave pública não é mais necessária.

O período criptográfico de uma chave privada utilizada para assinar documentos digitais geralmente é menor que o período criptográfico

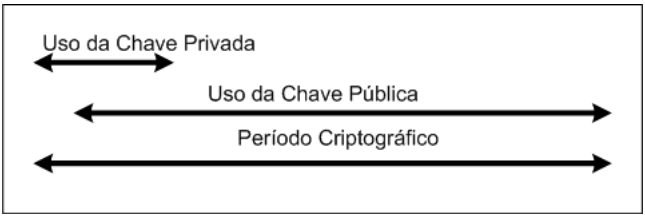


**Figura 2.1:** Tempo de uso de um par de chaves para assinatura digital

de sua respectiva chave pública. Neste caso, a chave privada é utilizada para gerar as assinaturas digitais, enquanto a chave pública é utilizada para verificar a validade da assinatura do documento. As chaves privadas geralmente são destinadas a utilização por um período fixo de tempo, depois deste tempo o proprietário da chave deveria destruí-la. A chave pública poderia ficar disponível por um longo período para verificação das assinaturas, só que existem outros fatores que devem ser considerados para limitar este período. A figura 2.1 apresenta este exemplo através de uma forma gráfica.

Algumas vezes o período criptográfico é definido por um período de tempo arbitrário, ou pela máxima quantidade de dados protegida pela chave. Porém, uma ótima escolha para um período criptográfico envolve a avaliação cuidadosa dos riscos e as consequências da exposição indevida de uma chave [1].

Alguns fatores que devem ser ponderados ao definir um período criptográfico, de acordo com [1], são:

- A força dos mecanismos criptográficos (algoritmos, tamanho de chaves, modo de operação dos algoritmos etc);
- O ambiente operacional (acesso controlado ao ambiente, acesso público via terminais etc);
- O volume de informações a ser protegida, ou o número de transações;
- O período de tempo em que os dados devem estar seguros;
- A função utilizada (cifragem de dados, assinatura de dados, proteção de chaves etc.);
- O método de recuperação da chave;
- O processo de atualização da chave, ou de derivação da chave;
- O número de nós em uma rede que compartilham a mesma chave;
- O número de cópias de uma chave, e a distribuição destas cópias;

- A ameaça à informação (contra quem a informação precisa ser protegida, quais as capacidades técnicas e financeiras que os atacantes tem para montar um ataque etc).

No geral, curtos períodos criptográficos aumentam a segurança. Por exemplo, alguns algoritmos criptográficos podem se tornar menos vulneráveis à criptoanálise, se o adversário possuir somente uma quantidade limitada de informação cifrada por uma chave específica [1].

### 2.4.1 Períodos Criptográficos Recomendados

Através do documento [1], são realizadas algumas recomendações de períodos criptográficos de acordo com a utilidade do par de chaves.

Se o par de chaves for utilizado para assinaturas digitais, o período criptográfico da chave privada geralmente é menor que o da chave pública correspondente. Segundo Barker et al [1], o período criptográfico máximo recomendado para as chaves privadas utilizadas para assinaturas digitais é entre 1 e 3 anos. Considerando que a chave em questão utilize algum dos algoritmos aprovados pelo FIPS, e que ela deve ser destruída após o período criptográfico. O período criptográfico para a chave pública pode ser definido na ordem de vários anos, todavia devido ao longo período de exposição, a confiabilidade de uma assinatura é reduzida com o passar do tempo.

Alguns sistemas utilizam a função de carimbo do tempo para atestar a data em que uma assinatura é válida. Com este mecanismo, mesmo quando o período criptográfico da assinatura expirar, ela pode ser validada, pois a chave pública desta entidade poderá ser utilizada para verificar a assinatura anterior, sendo que esta não está com o seu período criptográfico expirado.

Em pares de chaves utilizados para autenticação, geralmente, o período criptográfico é o mesmo para as chaves privada e pública. De acordo com [1], o período criptográfico máximo recomendado para ambas as chaves (privada e pública) é entre 1 e 2 anos, dependendo do ambiente aonde serão utilizadas e da sensibilidade (ou criticidade) das informações de autenticação.

## 2.5 CURVAS ELÍPTICAS

Em 1985, Neal Koblitz [**?**] e Victor Miller [**?**] propuseram o uso de curvas elípticas em criptografia. A partir deste trabalho, várias pesquisas foram publicadas, entretanto, somente a partir do final da década de 90 curvas elípticas receberam maior interesse comercial, quando começaram a surgir os primeiros padrões e protocolos [35].

A criptografia de curvas elípticas utiliza como base uma curva elíptica, que é definida através de uma série de parâmetros. Diferentes parâmetros formam diferentes curvas. Em criptografia, uma curva é definida sobre um conjunto de cinco parâmetros.

Existem vários critérios que devem ser considerados quando forem selecionados os parâmetros de uma curva elíptica para uma aplicação específica, os principais são:

1. Funcionalidade - Quais garantias são oferecidas para que o protocolo seja seguro?
2. Segurança - A chave pública provê a capacidade desejada?
3. Performance - Para o nível de segurança desejado, as implementações atingem os objetivos de performance?
4. Interoperabilidade - Se houver integração com outras aplicações, estas irão reconhecer a curva selecionada?

Através dos anos, diversas pesquisas foram feitas para assegurar a garantia dos protocolos criptográficos. O conceito fundamental que difere os algoritmos são as suas bases matemáticas. Alguns algoritmos são baseados em fatoração de números primos, como o RSA. Outros são baseados em logaritmos discretos, como o DSA. Outros ainda são baseados em logaritmos discretos com curvas elípticas, como o ECDSA. A diferença em sua base matemática é que estabelece o tamanho do domínio e das chaves, e estas possuem um impacto direto na performance das aplicações em que são utilizadas. Utilizando algoritmos que possuem várias pesquisas realizadas (como RSA, ECDSA etc), é possível satisfazer o primeiro critério citado anteriormente.

Todos os algoritmos criptográficos se baseiam na resolução de problemas matemáticos. Estes problemas podem ser solucionados, no entanto, se utilizados números grandes, estas soluções se tornam computacionalmente impraticáveis. Geralmente as soluções encontradas possuem complexidade polinomial. A ordem de grandeza destes números está relacionada com o tipo de problema a ser resolvido. Este é o motivo que algoritmos baseados em fatoração de números primos possuem chaves de tamanho maior que algoritmos baseados no problema do logaritmo discreto. O algoritmo mais rápido conhecido para fatorar números inteiros é o *Number Field Steve* (NFS), que possui complexidade exponencial. Até 2010, o maior módulo RSA fatorado foi um número de 232 dígitos (correspondente a 768 bits) em dezembro de 2009, utilizando vários computadores em paralelo, equivalentes a computação de 3.300 Opterons 1GhZ por 1 ano [36]. Para o problema de logaritmos discretos com curvas elípticas, o recorde atual é de 112bits (curva secp112r1), quebrado em julho de 2009.

Utilizando as soluções conhecidas para resolver os problemas bases dos algoritmos criptográficos, importantes entidades, como o NIST, conseguem mensurar a equivalência de força entre os algoritmos para diferentes tamanhos de chaves. A tabela 2.1 da seção 2.3 apresenta a equivalência de força entre diferentes algoritmos.

Através da escolha do tamanho correto da chave (veja seção 2.3 para mais detalhes), é possível assegurar que o par de chaves satisfaz o segundo critério, citado no começo desta seção.

| Nome da Curva | Força | Tamanho Chave | Koblitz / Aleatório | SECG | NIST | RFC 5480 | NSA Suite B |
|---|---|---|---|---|---|---|---|
| secp192k1 | 96 | 192 | Koblitz | X | | | |
| secp192r1 | 96 | 192 | Aleatório | X | X | X | |
| secp224k1 | 112 | 224 | Koblitz | X | | | |
| secp224r1 | 112 | 224 | Aleatório | X | X | X | |
| secp256k1 | 128 | 256 | Koblitz | X | | | |
| secp256r1 | 128 | 256 | Aleatório | X | X | X | X |
| secp384r1 | 192 | 384 | Aleatório | X | X | X | X |
| secp521r1 | 256 | 521 | Aleatório | X | X | X | |

**Tabela 2.4:** Curvas elípticas de corpos primos recomendadas pelo SECG, NIST, RFC5480 e NSA Suite B

Além do tamanho da chave utilizada, é importante selecionar uma curva que tenha uma boa performance. Diversas entidades (como por exemplo NIST, SECG etc) recomendam o uso de determinadas curvas. Estas curvas, além de utilizarem número primos específicos que são escolhidos especialmente para facilitar a otimização da implementação dos algoritmos, foram padronizadas para facilitar a interoperabilidade entre aplicações [37].

O SECG recomenda 8 curvas elípticas para corpos primos, e 12 para corpos binários, que são apresentados respectivamente nas tabelas 2.4 e 2.5.

A primeira coluna das tabela 2.4 apresenta o nome das curvas. Estes nomes foram atribuídos no documento [37]. As segunda e terceira coluna informam a força e o tamanho das chaves geradas a partir dos parâmetros destas curvas. A quarta coluna indica se os parâmetros da curva estão associados com a curva de Koblitz, ou se foram escolhidos aleatoriamente. As quatro últimas colunas definem se estas curvas são recomendadas pelos padrões estabelecidos pela SECG, NIST, RFC5480[1], NSA Suite B e ANSI X9.62, respectivamente.

As colunas da tabela 2.5 possuem o mesmo significado das colunas

[1] A RFC5480 lista 15 curvas, porém por questões de interoperabilidade entre aplicações, são recomendadas somente 5. Nesta tabela somente foram consideradas estas últimas.

| Nome da Curva | Força | Tamanho Chave | Koblitz / Aleatório | SECG | NIST | RFC 5480 | NSA Suite B |
|---|---|---|---|---|---|---|---|
| sect163k1 | 80 | 163 | Koblitz | X | X | | |
| sect163r1 | 80 | 163 | Aleatório | X | | | |
| sect163r2 | 80 | 163 | Aleatório | X | X | | |
| sect233k1 | 112 | 233 | Koblitz | X | X | | |
| sect233r1 | 112 | 233 | Aleatório | X | X | | |
| sect239k1 | 115 | 239 | Koblitz | X | | | |
| sect283k1 | 128 | 283 | Koblitz | X | X | | |
| sect283r1 | 128 | 283 | Aleatório | X | X | | |
| sect409k1 | 192 | 409 | Koblitz | X | X | | |
| sect409r1 | 192 | 409 | Aleatório | X | X | | |
| sect571k1 | 256 | 571 | Koblitz | X | X | | |
| sect571r1 | 256 | 571 | Aleatório | X | X | | |

**Tabela 2.5:** Curvas elípticas de corpos binários recomendadas pelo SECG, NIST, RFC5480 e NSA Suite B

da tabela 2.4. Elas foram separadas para diferenciar as curvas que utilizam corpos primos e as que utilizam corpos binários.

Vale ressaltar que as normas RFC5480, NSA Suite B e ANSI X9.62 não recomendam o uso de curvas elípticas de corpos binários.

A nomenclatura das curvas é diferente nos diversos padrões apresentados neste trabalho. A tabela 2.6 apresenta a nomenclatura destas curvas definidas pelos padrões SECG, NIST e ANSI X9.62.

## 2.6 CONCLUSÃO

Este capítulo apresentou uma visão geral dos requisitos que devem ser considerados ao selecionar uma chave para uma determinada

| SECG | ANSI X9.62 | NIST |
|---|---|---|
| sect163k1 | | NIST K-163 |
| sect163r1 | | |
| sect163r2 | | NIST B-163 |
| sect193r1 | | |
| sect193r2 | | |
| sect233k1 | | NIST K-233 |
| sect233r1 | | NIST B-233 |
| sect239k1 | | |
| sect283k1 | | NIST K-283 |
| sect283r1 | | NIST B-283 |
| sect409k1 | | NIST K-409 |
| sect409r1 | | NIST B-409 |
| sect571k1 | | NIST K-571 |
| sect571r1 | | NIST B-571 |
| secp160k1 | | |
| secp160r1 | | |
| secp160r2 | | |
| secp192k1 | | |
| secp192r1 | prime192v1 | NIST P-192 |
| secp224k1 | | |
| secp224r1 | | NIST P-224 |
| secp256k1 | | |
| secp256r1 | prime256v1 | NIST P-256 |
| secp384r1 | | NIST P-384 |
| secp521r1 | | NIST P-521 |

**Tabela 2.6:** Nomenclatura de curvas elípticas com mesmos parâmetros sobre diferentes padrões

aplicação. Também foi feito um comparativo da força de chaves criadas utilizando diferentes algoritmos. Pode-se concluir que as chaves que utilizam algoritmos baseados na resolução do problema do logaritmo discreto com curvas elípticas possuem maior força, se comparadas com chaves de mesmo tamanho que utilizam algoritmos baseados na fatoração de números primos. Isto é um ponto muito importante para o desenvolvimento de aplicações que possuem requisitos de performance, ou que possuem recursos computacionais limitados. Ao final do capítulo foi feito uma breve introdução sobre as teorias matemáticas que servem de base para o entendimento de criptografia de curvas elípticas. Por último, foram apresentadas as curvas recomendados pelas mais importantes organizações, responsáveis por definir diversos padrões em criptografia.

# 3 FUNDAMENTOS DE ICP

## 3.1 INTRODUÇÃO

Este capítulo visa introduzir ao leitor conceitos necessários para o entendimento deste trabalho. Inicialmente serão apresentados alguns conceitos mais básicos, como Autoridade Certificadora (AC), certificado auto-assinado etc. Também serão explanados alguns conceitos técnicos e realizadas algumas definições acerca da nomenclatura adotada no trabalho. Por último, é apresentado um breve resumo sobre as principais técnicas de integração existentes na literatura.

## 3.2 IDENTIFICADOR DE OBJETO

Um Identificador de Objeto (OID) é um número utilizado para identificar um objeto, seja ele real ou virtual. Estruturalmente, um OID representa um nodo em uma árvore hierárquica. Um OID representa o caminho necessário para chegar até um nodo específico, utilizando uma busca em profundidade. Cada passo deste caminho é separado pelo caractere ponto (.) A figura 3.1 apresenta uma hierarquia de OIDs fictícios.

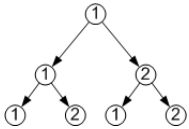


**Figura 3.1:** Estrutura Hierárquica OID

Os nodos folhas poderiam ser representados da esquerda para a direita, respectivamente por 1.1.1, 1.1.2, 1.2.1 e 1.2.2. O primeiro OID (1.1.1) partiria do nodo raiz (1), iria para o nodo 1, da esquerda (1.1), depois para o nodo 1, novamente a esquerda (1.1.1).

Os OIDs são padronizados por um órgão chamado Internet Assigned Numbers Authority (IANA), e qualquer organização pode solicitar um OID. Como os OIDs possuem uma estrutura hierárquica, o IANA somente registra que um determinado ramo pertence a uma determinada organização, a partir daquele ponto a organização é responsável pela distribuição dos OIDs para aquele ramo.

## 3.3 CERTIFICADOS DIGITAIS

Um certificado digital, serve para identificar a chave pública de um indivíduo ou entidade. Um certificado é composto por alguns atributos, chamados atributos básicos. Estes atributos caracterizam a identificação

do usuário do certificado. Além destes atributos, um certificado pode conter informações adicionais, chamadas de extensões, que podem assumir diversas estruturas. Algumas extensões são padronizadas pela RFC5280 [3], mas, novas extensões podem ser criadas de acordo com a necessidade de determinada organização. Vale ressaltar que a criação de novas extensões pode comprometer a interoperabilidade do certificado.

Um certificado digital pode ser classificado em duas classes: Certificados de entidade finais, e certificados de ACs. Os certificados de ACs podem ser subdivididos em três classes: Certificado Cruzado, Certificado auto-emitido e Certificado auto-assinado [3].

Certificados cruzados são os certificados em que o emissor e o sujeito são diferentes ACs. Certificados cruzados descrevem uma relação de confiança entre duas ACs [3]. Em hierarquias de ICP, a AC que emite o certificado de uma AC subordinada é chamada de AC Superior [38]. Uma certificação cruzada pode ser unilateral ou bilateral [31].

Um certificado auto-emitido (*self-issued*) é um certificado em que o emissor e o sujeito do certificado são a mesma entidade. Geralmente este tipo de certificado é utilizado para suportar a troca de políticas, ou operações [3]. Quando em um certificado o emissor e o sujeito possuem o mesmo Domain Name (DN), porém as chaves são diferentes, este é chamado de *rollover certificates* ou *key rollover*. Este tipo de certificado geralmente é utilizado quando há troca do par de chaves da entidade, e se caracteriza pela emissão de um certificado para o novo par de chaves assinado pelo velho, e um certificado para o velho par de chaves assinado pelo novo.

Certificados auto-assinados (*self-signed*) são certificados auto-emitidos, em que a assinatura do certificado pode ser verificada através da chave pública que está contida no certificado [3]. Estes certificados são utilizados para facilitar a distribuição de uma chave pública, e geralmente utilizados em Autoridades Certificadoras Raízes. Estas, por sua vez, normalmente representam o ponto de confiança dos usuários.

Certificados de entidades finais são certificados emitidos para entidades que não tem autorização de emitir certificados. Estes certificados geralmente pertencem a usuários, computadores, equipamentos etc e popularmente também são conhecidos como certificados de usuários finais.

## 3.4 INFRAESTRUTURA DE CHAVES PÚBLICAS

Nesta seção serão apresentados alguns conceitos necessários para o entendimento deste trabalho. Também serão apresentadas algumas definições para que diferentes públicos tenham o mesmo entendimento sobre o assunto.

### 3.4.1 Autoridade Certificadora Principal

Quando uma ICP pretende se associar a outra ICP, formando um novo domínio, estas devem eleger uma AC para gerenciar as relações de confiança com as outras infraestruturas do domínio [31]. A AC Principal não precisa ser uma AC criada especificamente para esta finalidade, podendo exercer esta função simultaneamente com a de emissão de certificados para usuários. A AC pode ser definida como qualquer AC pertencente a ICP, incluindo o ponto de confiança.

### 3.4.2 Arquiteturas de ICP

Uma ICP pode ser formada por uma ou mais Autoridades Certificadoras. Dentre estas, no mínimo uma deve ser definida como sendo a âncora de confiança (ou ponto de confiança).

A combinação destas ACs em estruturas pode ser realizada através de quatro arquiteturas: Única AC, Hierárquica, Malha, Híbrida; que serão detalhadas nas seções a seguir.

#### 3.4.2.1 Única AC

A arquitetura de Única AC é a mais simples de todas, compreendendo apenas uma única AC, que emite certificados para todos os usuário da ICP. O certificado desta AC é auto-assinado, e como é a única AC pertencente a infraestrutura, também é o ponto de confiança das entidades finais. A figura 3.2 apresenta uma ICP com arquitetura de Única AC.

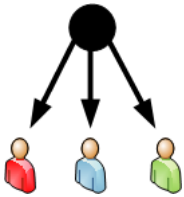

**Figura 3.2:** Arquitetura de ICP: Única AC

#### 3.4.2.2 Hierárquica

Uma ICP com estrutura hierárquica consiste em uma única AC com certificado auto-assinado, chamada AC Raiz, que emite certificados para um ou mais níveis de ACs subordinadas [8]. E, estas emitem certificados para os usuários. A figura 3.3 apresenta um exemplo desta arquitetura.

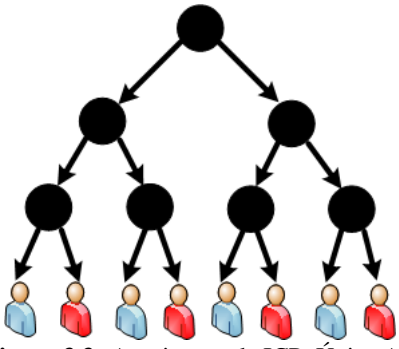

**Figura 3.3:** Arquitetura de ICP: Única AC

#### 3.4.2.3 Malha

A estrutura em malha caracteriza-se pela existência de múltiplas ACs com certificados auto-assinados. A relação entre as ACs é feita através da emissão de certificados cruzados entre estas [8]. Uma das principais vantagens desta abordagem é a redundância de caminhos de certificação. Todavia, esta arquitetura permite a criação de ciclos, que podem dificultar a montagem do caminho de certificação, caso o algoritmo não consiga detectá-los.

A figura 3.4 demonstra um exemplo deste modelo. Nesta figura,

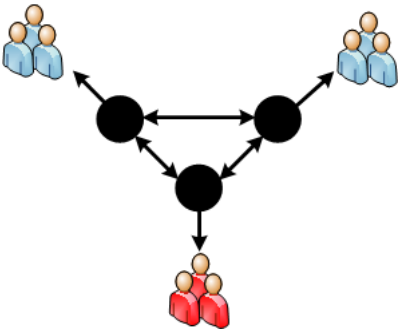

**Figura 3.4:** Arquitetura de ICP: Malha

todas as ACs emitiram certificados cruzados com todas as outras ACs, caracterizando uma arquitetura de malha completa. Nesta, o principal benefício é que o ponto de confiança pode ser alcançado através de apenas um certificado, diminuindo a complexidade de montagem do caminho de certificação. Uma ICP que adota a arquitetura de malha, mas nem todas as ACs emitem certificados cruzados para todas as outras ACs, utiliza a arquitetura de malha parcial. Nesta, um caminho de certificação pode não existir entre duas ACs específicas.

O ponto de confiança dos usuários nestas arquiteturas pode ser a própria AC que emitiu o seu certificado, ou pode ser outra AC, pertencente à ICP, definida pelo administrador da ICP.

#### 3.4.2.4 Híbrida

Uma ICP que adota a arquitetura híbrida é aquela que utiliza a combinação das arquiteturas mostradas anteriormente (Única AC, hierárquica e malha).

A âncora de confiança nesta arquitetura geralmente é a AC Raiz, no entanto, devido a complexidade que uma ICP com arquitetura híbrida pode ter, pode ser escolhida outra AC para ponto de confiança. Recomenda-se que os administradores das infraestruturas que utilizam esta arquitetura tenham o cuidado de orientar cuidadosamente os usuários na correta definição da âncora de confiança, pois a incorreta escolha por um usuário, dependendo da estrutura adotada, pode inviabilizar a montagem do caminho de certificação.

A figura 3.5 demonstra uma ICP utilizando a arquitetura híbrida.

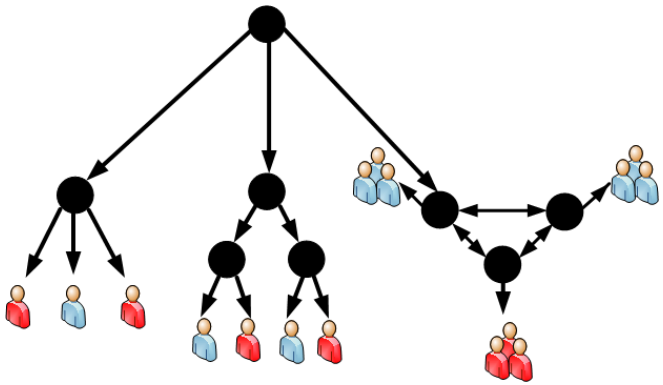

**Figura 3.5:** Arquitetura de ICP: Híbrida

### 3.4.3 Ponto de Atualização

Segundo Carlos[39], ponto de atualização pode ser definido como sendo o momento no tempo em que um certificado de AC precisa ser atualizado. Este momento ocorre quando a AC não pode emitir mais certificados digitais pelo fato de seu tempo de validade restante ser inferior ao período de validade que ela atribui aos certificados que emite.

Por exemplo, seja uma AC que possui validade de dez anos, e emite certificados com validade de três anos. Esta AC, no primeiro dia após completar sete anos, não poderá mais emitir novos certificados, pois estes irão ultrapassar a data de validade do certificado da própria AC. Esta data é definida como sendo o ponto de atualização.

### 3.4.4 Caminho de certificação

Um certificado digital somente é considerado válido se os os seus dados forem validados por uma terceira parte confiável, a âncora de confiança. Em uma ICP, a âncora de confiança pode delegar a emissão de certificados digitais a outras ACs. E, para verificar a identidade destas ACs, é necessário existir um caminho de certificação entre o certificado a ser validado e o ponto de confiança do usuário. Assim, a confiança depositada pelo usuário no ponto de confiança é propagada até o certificado validado.

Segundo a RFC5217 [31], um caminho de certificação pode ser definido como sendo uma sequência ordenada de certificados em que o sujeito de um certificado é o emissor do próximo certificado da sequência. O caminho de certificação começa com o certificado de uma âncora de confiança e termina com o certificado de uma entidade final [3].

Apesar de não ser um processo padronizado e com poucas referências na literatura, de um modo geral o processamento do caminho de certificação consiste em duas etapas: Construção e Validação. Na primeira etapa são montados os possíveis caminhos, e na segunda são feitas diversas verificações nos possíveis caminhos, como situação da revogação, datas de validade, integridade, restrições nomes, restrições políticas, extensões etc. Caso alguma destas validações falhar, o caminho é descartado. Se um dos caminho gerados na primeira etapa for validado com sucesso, então os certificados deste caminho de certificação são considerados válidos.

A norma RFC5280 [3] especifica um algoritmo sugerido para ser utilizado na montagem e validação do caminho de certificação, mas é definido que este algoritmo não precisa ser utilizado. Porém, quando outro algoritmo for utilizado, ele deve exibir os mesmos resultados que o algoritmo sugerido na norma.

Quando o certificado auto-assinado de uma AC Raíz é utilizado para distribuir as informações do ponto de confiança, os conteúdos das extensões deste certificado pode ser utilizado como valores iniciais recomendados para o algoritmo de validação do caminho de certificação. As implementações que utilizarem certificados auto-assinados para especificar informações do ponto de confiança são livres para determinar se irão utilizar estas informações [3].

No algoritmo de validação do caminho de certificação descrito na RFC5280 [3], a validação do caminho de certificação não inclui a validação das informações do certificado do ponto de confiança, nem especifica regras para a validação das extensões deste certificado. Naquele algoritmo, o certificado do ponto de confiança é utilizado apenas para a distribuição da chave pública, que é o único parâmetro inicial do algoritmo que é proveniente do certificado do ponto de confiança. Sendo assim, neste trabalho ao utilizar o termo caminho de certificação, estaremos nos referindo aos certificados compreendidos entre o certificado da entidade final e o certificado a AC subordinada ao ponto de confiança.

### 3.4.5 Extensão Authority Information Access

A extensão Authority Information Access (AIA) é uma extensão que pode ser utilizada em certificados digitais ou LCRs.

Ela especifica como acessar informações e serviços do emissor de um certificado ou do emissor de uma LCR. Essas informações e serviços podem incluir serviços de validação online ou dados da AC. Esta extensão não deve conter informações da localização da LCR, pois esta é especificada na extensão CRL Distribution Points.

As ACs que seguem as recomendações da RFC 5280 devem marcar esta extensão como não crítica.

Esta extensão é formada por uma sequência de Descritores de Acesso. Cada Descritor de Acesso é formado por dois parâmetros:

- Método de Acesso: Este parâmetro descreve qual o tipo da informação. Este parâmetro é constituído por um OID;
- Local de Acesso: Este parâmetro descreve a localização da informação.

O mecanismo (HTTP, HTTPS, FTP, LDAP etc.) utilizado para buscar uma informação pode ser determinado implicitamente pelo Método de Acesso, ou explicitamente pelo Local de Acesso.

A RFC5280 apresenta dois Métodos de Acesso:

- CA issuers(id-ad-caIssuers): Lista o(s) certificado(s) da Autoridade Certificadora que emitiu o certificado que possui a extensão AIA;
- OCSP(id-ad-ocsp): Lista o(s) endereço(s) do(s) serviço(s) OCSP disponível (eis).

Estes Métodos de Acesso serão detalhados nas próximas seções.

#### 3.4.5.1 CA issuers(id-ad-caIssuers)

Quando for utilizado o Método de Acesso *CA issuers* na extensão AIA, este serve para indicar a localização do(s) certificado(s) da AC que emitiu o certificado que contém a extensão.

O objetivo principal deste Método de Acesso é facilitar a montagem do caminho de certificação até o ponto de confiança do usuário.

Quando o Método de Acesso utilizado for *CA issuers*, o parâmetro Local de Acesso deve conter o endereço para o serviço, e descrever qual o protocolo utilizado. O parâmetro Local de Acesso é um GeneralName, e pode conter vários formatos.

Um dos formatos do parâmetro Local de Acesso, é um Identificador de Recursos Uniforme (URI) apontando para o(s) certificado(s) da AC. Se este formato for utilizado, a URI deve conter o protocolo (FTP, HTTP, LDAP etc) utilizado para buscar as informações. Se esta URI apontar apenas para um certificado, ele deve estar codificado em DER.

Se apontar para um grupo de certificados, que podem estar codificados em uma mensagem CMS, conforme especificado em [40].

A extensão AIA pode especificar diversos *CA issuers*, que podem apontar para as mesmas informações, ou para informações diferentes, mas pelo menos um dos métodos de acesso deve apontar para uma URI HTTP ou LDAP.

#### 3.4.5.2 OCSP(id-ad-ocsp)

O Método de Acesso *OCSP* é utilizado quando as informações de revogação estão disponíveis através de um serviço *Online Certificate Status Protocol* (OCSP).

Neste Método de Acesso o parâmetro Local de Acesso deve conter a localização do servidor OCSP. Esta localização deve conter o protocolo utilizado, e o endereço para encontrar o servidor [41]. Um exemplo de endereço, seria a URL *http://www.ac-teste.com.br/servidor-ocsp*. Esta URL contém o protocolo (HTTP) e o endereço do servidor (www.ac-teste.com.br/servidor-ocsp).

### 3.4.6 Assinaturas Digitais

A geração da assinatura digital de um documento é feita através da cifragem do resultado de uma função resumo aplicada a um determinado documento, utilizando a chave privada do assinante. A figura 3.6 apresenta este processo.

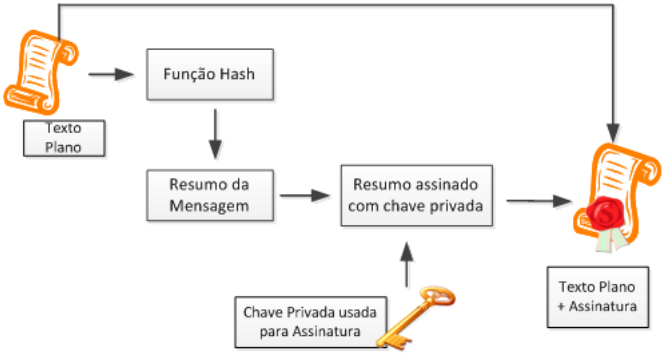


**Figura 3.6:** Geração de Assinatura Digital

A validação de um documento assinado digitalmente é realizada através da validação do certificado do assinante, e após, a validação da assinatura. A primeira etapa de validação consiste em verificar a autenticidade e validade da chave do usuário assinante. Esta etapa compõe-se da construção e validação do caminho de certificação (ver seção 3.4.4) entre

o certificado do signatário e algum ponto de confiança do usuário que está validando a assinatura.

A segunda etapa está associada ao algoritmo criptográfico que foi utilizado na assinatura digital, e o seu processo de verificação de integridade. Este é realizado de forma inversa ao processo de geração da assinatura, conforme descrito na figura 3.7. A assinatura gerada é deci-

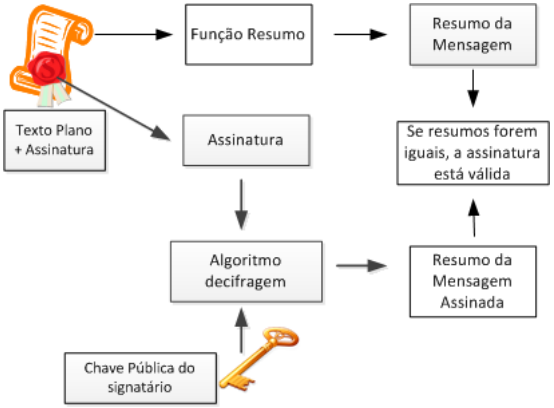


**Figura 3.7:** Validação de Assinatura Digital

frada com a chave pública do assinante, e o resultado é comparado com o resultado da função resumo aplicada ao documento a ser verificado. Este processo garante que o documento não sofreu modificações posteriores à sua assinatura, e que esta foi produzida pela chave privada correspondente a chave pública utilizada para verificar a assinatura.

Uma assinatura pode ser válida em determinado momento, e depois tornar-se inválida. Isto deve-se ao fato que a validade dos certificados digitais pode mudar ao longo do tempo. A figura 3.8 demonstra como a validade de uma assinatura digital pode mudar ao longo do tempo,

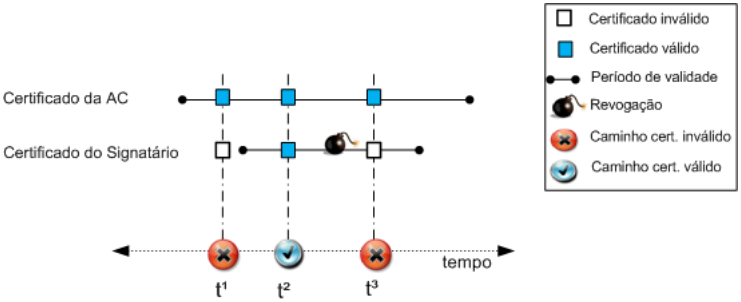


**Figura 3.8:** Validação de Assinatura Digital

considerando a validade dos certificados de um determinado caminho de

certificação.

No tempo $t1$, a assinatura foi gerada antes da data de validade inicial de um dos certificados do caminho de certificação; assinatura inválida. Em $t2$, todos os certificados estão válidos; assinatura válida. Em $t3$, um dos certificados foi revogado anteriormente; assinatura inválida.

Segundo [42], quando não há uma referência ao momento em que a assinatura digital foi criada, é recomendável que a referência utilizada para verificar a assinatura seja a data em que a verificação é realizada. A justificativa para tal está na consulta à última situação de revogação dos certificados, evitando assim desconsiderar uma revogação recente.

Através da figura 3.8, é possível verificar que mesmo uma assinatura válida, após determinado tempo, perde sua validade. Se um certificado do caminho de certificação for revogado, a validade da assinatura também é perdida, mesmo se a revogação ocorrer após a geração da assinatura. Para atestar de forma confiável a data em que uma assinatura foi realizada, além de prolongar a sua validade, foi criado um mecanismo chamado de Carimbo do Tempo, descrito na próxima seção.

### 3.4.7 Carimbo do Tempo

Durante a validação de assinaturas digitais é necessário estabelecer a data em que estas foram geradas. Isto pode ser realizado através de um serviço chamado carimbo do tempo. Este serviço possui a propriedade de garantir a existência de um documento em determinada data.

Para associar uma data a algum documento, de forma confiável, faz-se o uso de uma terceira parte confiável chamada Autoridade de Carimbo do Tempo (ACT). A esta, está associado um relógio sincronizado com uma fonte de tempo confiável. Desta maneira, a ACT pode emitir carimbos do tempo assinados que comprovam que um determinado conteúdo já existia na data de emissão destes carimbos.

Segundo [43], a ACT pode ser utilizada para indicar que uma assinatura foi aplicada a uma mensagem antes do certificado correspondente ser revogado, permitindo assim que um certificado revogado possa ser utilizado para verificar assinaturas feitas antes da sua revogação.

Para validar uma assinatura digital com carimbo do tempo, o verificante primeiramente valida o carimbo do tempo com base na data atual, e depois, é feita a validação da assinatura digital considerando a data presente no carimbo do tempo. Desta maneira, o caminho de certificação do carimbo do tempo é montado com os estados atuais de revogação, garantindo que as informações prescritas pelo carimbo são verdadeiras.

A ACT, desta maneira, permite que após a expiração ou revogação do certificado do usuário consiga-se identificar uma assinatura válida, realizada antes do incidente.

Entretanto após determinado período, o carimbo na ACT irá expirar, fazendo com que o caminho de certificação do carimbo do tempo torne-se inválido. Para contornar esta limitação, emite-se um novo ca-

rimbo do tempo sobre o carimbo anterior. A figura 3.9, retirada de [42], apresenta este procedimento. Na figura 3.9, a assinatura digital foi criada em $t_{sig}$, tempo em que o caminho de certificação é válido. No tempo

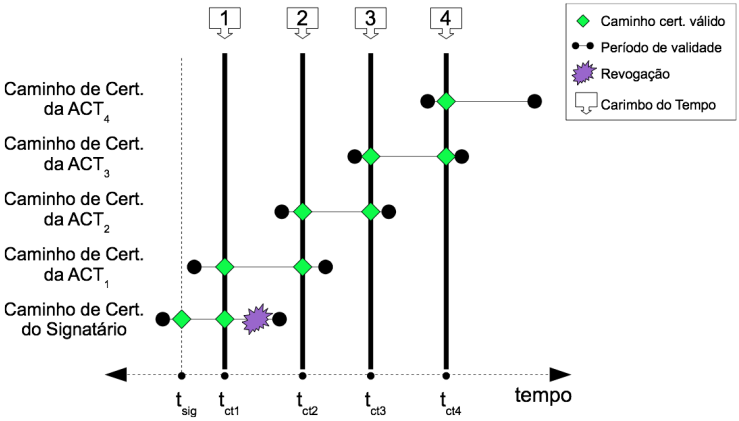


**Figura 3.9:** Carimbo do Tempo

$t_{ct1}$ é emitido um carimbo para esta assinatura, postergando a sua validade. Em $t_{ct1}$ o certificado os caminhos de certificação do signatário e da $\text{ACT}_1$ devem ser válidos. Em $t_{ct2}$, a validade do carimbo emitido em $t_{ct1}$ é postergada. O mesmo processo é repetido em $t_{ct3}$ e $t_{ct4}$ para postergar a validade destes carimbos.

O processo de verificação desta assinatura é feito através da validação do último carimbo $t_{ct4}$ com base na data atual. Depois é validado o carimbo $t_{ct3}$ com base na data descrita no carimbo $t_{ct4}$. Este processo é repetido até chegar a assinatura digital, que é validada com base na data presente no carimbo do tempo emitido em $t_{ct1}$.

## 3.5 ELEMENTOS DE CONFIANÇA

Em um ambiente ideal, todos os usuários de ICP iriam compartilhar apenas um ponto de confiança. Por questões de confiabilidade no mundo real isto é impraticável. Diferentes organizações possuem opiniões variadas. Há também o aspecto da confiança, quando as informações protegidas são muito valiosas. Por exemplo, uma ICP desenvolvida para tratar dos aspectos militares de um país não vai querer compartilhar o mesmo ponto de confiança que outros militares de outros países. Cada um vai querer possuir o controle do seu próprio ponto de confiança. Outro aspecto que cria a necessidade de segmentação de ICPs é o objetivo primário das ICPs. Uma ICP pode ter o objetivo de autenticar usuário e reconhecer assinaturas digitais com eficácia probante, enquanto outra ICP pode somente querer divulgar a tecnologia e utiliza-la mais informalmente, sem eficácia probante.

Através dessa necessidade, criam-se várias ICPs. Algumas necessitam trocar informações entre si, umas apenas por um determinado período de tempo, outras por um tempo indeterminado. Nessas condições, surgem alguns mecanismos para possibilitar a comunicação e validação de assinaturas entre diferentes ICPs.

Ao introduzir esse conceito de comunicação entre diferentes ICPs, cria-se a necessidade de gerenciar essa comunicação (quais ICPs serão confiáveis, como serão validados os documentos assinados pelas outras ICPs etc). As próximas seções deste capítulo apresentam alguns modelos de integração de ICPs e explicam como é o seu respectivo gerenciamento. Também são apresentados os benefícios e limitações de cada uma das alternativas. Ao final, são feitas sugestões sobre ambientes para as quais cada uma das soluções apresentadas são mais adequadas.

Esta seção apresenta diferentes maneiras de criar relações de confiança entre ICPs. Também apresenta algumas considerações necessárias para a implementação destas relações entre ICPs, e identifica aspectos que podem ser implementados para facilitar a criação de relações de confiança para integração de ICPs.

### 3.5.1 Integração de ICPs com mecanismos externos

A integração de ICPs pode ser realizada através de mecanismos externos, sem haver a necessidade de alteração da infraestrutura.

A utilização destes mecanismos para integrar ICPs pode ser feita sem a necessidade de conhecimento da integração pela infraestrutura [31]. Ou seja, as ICPs que estão integradas a partir de mecanismos externos podem não saber que fazem parte de um determinado domínio, criado pela parte confiante.

#### 3.5.1.1 Listas de Certificados Confiáveis

A maneira mais simples de integrar diferentes ICPs é o usuário possuir uma Lista de Certificados Confiáveis (LCC) [8]. Segundo [31], uma lista de certificados confiáveis é um conjunto de âncoras de confiança, utilizado para confiar em uma ou mais ICPs. Esta lista contém os certificados que o usuário julga serem confiáveis. A grande vantagem desde mecanismo é a simplicidade, para um usuário adicionar novas ACs confiáveis, o usuário apenas precisa inserir o certificado nesta lista. Esta é uma solução bastante simples, mas possui limitações:

- Ao inserir um certificado na lista de certificados confiáveis, o usuário precisa investigar se o certificado é confiável;
- O usuário deve manter e atualizar informações críticas sobre cada uma das ACs presentes na LCC. Conforme [44], geralmente as informações de acesso das ACs não são publicadas nos seus sítios

oficiais, nem mesmo os dados básicos, como URLs de acesso a repositórios e serviços. Isto pode causar uma extrema dificuldade para o usuário atualizar as informações sobre cada entidade. Segundo [44], o problema da falta de informações de acesso pode gerar ainda mais dificuldade se o usuário que precisa verificar as informações de uma determinada entidade não pertencer àquela organização (ou não tiver o seu certificado emitido por aquela entidade), pois este usuário terá acesso a informações limitadas;

- Geralmente quando há o comprometimento de uma AC, os usuários que tiveram seus certificados emitidos por aquela AC são comunicados. Todavia como o usuário não possui nenhum certificado emitido pela AC comprometida, ela não terá conhecimento que o usuário confia nela, e ele não será notificado sobre o comprometimento da AC. Este, então, vai continuar confiando na AC até descobrir a notícia do comprometimento;

- Quanto maior o número de ACs, mais difícil se torna o controle;

- A montagem do caminho de certificação fica mais complexa, pois existem várias ACs como pontos de confiança.

#### 3.5.1.2 Autoridade de Confiança

A manutenção de LCC pode ser feita localmente pelo usuário, ou através de uma terceira parte confiável. Esta terceira parte é chamada de Autoridade de Confiança (ACC).

Esta AC não emite certificados para outras ACs ou usuários, ela apenas é utilizada para assinar listas contendo certificados de ACs. O usuário então, passa a utilizar esta lista, que determina quais são os seus pontos de confiança. Neste modelo, o usuário deixa de confiar em várias ACs e a Autoridade de Confiança passa ser o seu ponto de confiança. É necessário tê-la como confiável (na lista local do usuário) para poder validar a assinatura da lista emitida pela Autoridade de Confiança. A distribuição desta lista não é padronizada, entretanto geralmente é feita através de repositórios HTTP, ou diretórios LDAP.

A figura 3.10 apresenta o funcionamento de uma Autoridade de Confiança. Na figura 3.10, os usuários possuem uma LCC local, em que a Autoridade de Confiança está presente, marcada como confiável. Com isto, a Autoridade de Confiança possui o poder de emitir LCCs para os usuários, que vão confiar indiretamente nas ACs presentes na LCC emitida por ela.

#### 3.5.1.3 Autoridade Unificadora

Esta técnica de integração é a mais simples, e consiste na criação de uma nova Autoridade Certificadora, que emite certificados para os Pontos

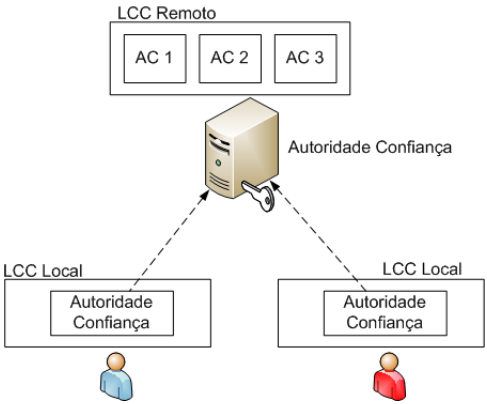


**Figura 3.10:** Autoridade de Confiança

de Confiança das ICPs a serem integradas. Sendo assim, estas começam a fazer parte de uma nova ICP, tendo como ponto de confiança esta nova AC.

A criação de uma nova AC, e modificação do ponto de confiança para esta AC, pode ser vista como a criação de uma nova ICP. Por este motivo, esta não será considerada um método de integração, mas será considerado como a criação de uma nova ICP com estrutura hierárquica.

A principal desvantagem deste método, está relacionado com a sua concepção, em que é necessário os usuários adotarem a AC Unificadora como ponto de confiança. Assim, esta AC torna-se o ponto de confiança para todos os usuários do domínio.

### 3.5.2 Integração de ICPs através de domínios

Além da integração através de mecanismos externos, existem os modelos de integração por domínios. Estes modelos são caracterizados pela necessidade de emissão de novos certificados digitais para integrar ICPs. Segundo a RFC5217 [31], relações de confiança são tecnicamente formalizadas pela emissão de certificados cruzados. As próximas seções explicam um pouco mais dos dois principais mecanismos: certificação cruzada e ponte.

#### 3.5.2.1 Certificação Cruzada

A certificação cruzada é uma relação de confiança mútua entre duas ACs. A figura 3.11 demonstra o esquema de certificação cruzada entre duas ACs. A AC1 emite um certificado para a AC2 (representado pela linha pontilhada na figura 3.11), e vice-versa. Quando a AC1 emite um certificado para a AC2, ela está “incorporando”em sua árvore todos os certificados emitidos pela AC2. O mesmo acontece com a AC2, através

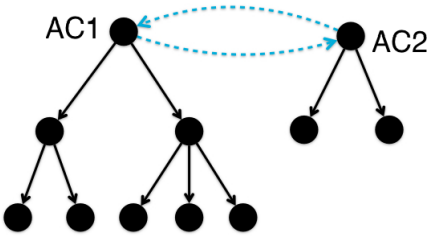


**Figura 3.11:** Certificação cruzada entre duas entidades

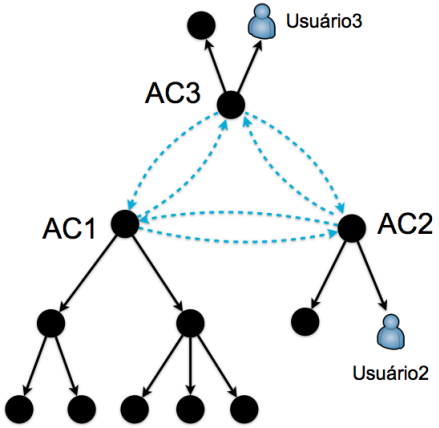


**Figura 3.12:** Certificação cruzada entre três entidades

do certificado que esta emitiu para a AC1.

A maior vantagem desta alternativa é que o usuário não é mais responsável por gerenciar quais as ACs confiáveis. Este papel é transferido para o administrador da AC, que deve verificar as políticas e práticas da outra AC antes de emitir o certificado. Além de diminuir o trabalho do usuário, o administrador da AC, geralmente, é mais qualificado para avaliar se uma AC é confiável ou não [8].

Quando houver o comprometimento da AC, apenas o administrador necessita ser comunicado. Ele revoga o certificado da AC, e esta ação faz com que aquela AC não seja mais confiável para todos os usuário da ICP. Nas LCCs, cada usuário precisa remover o certificado da AC comprometida.

A montagem do caminho de certificação fica mais simples, pois, há somente um ponto de confiança. Contudo se existirem 3 ou mais ACs realizando certificação cruzada entre si, háverão vários caminhos de certificação diferentes, e determinar o caminho mais curto pode tornar-se uma tarefa complicada. A figura 3.12 demonstra um exemplo de certificação cruzada entre 3 entidades. Para o usuário 2 validar o certifi-

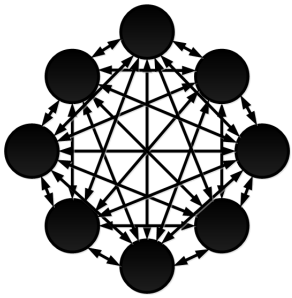

**Figura 3.13:** Certificação cruzada entre oito entidades

cado do usuário 3, os caminhos possíveis são: usuário 2 $\rightarrow$ AC2 $\rightarrow$ AC1 $\rightarrow$ AC3 $\rightarrow$ usuário 3 ou, usuário 2 $\rightarrow$ AC2 $\rightarrow$ AC3 $\rightarrow$ usuário 3. O aumento do número de ACs, que estabelecem relacionamentos de confiança entre si através de certificação cruzada, é diretamente proporcional ao aumento da complexidade de montagem do caminho de certificação.

Esta abordagem é uma solução apropriada somente quando houver um pequeno número de ACs estabelecendo relações de confiança, pois a cada nova relação de confiança é necessário emitir dois novos certificados. O número de relações necessárias é dado pela fórmula 3.1, e a quantidade de certificados é dada pela fórmula 3.2, onde $n$ é o número ACs que vão fazer a certificação cruzada.

$$\frac{n^2 - n}{2} \tag{3.1}$$

$$n^2 - n \tag{3.2}$$

A figura 3.13 apresenta um exemplo de certificação utilizada entre oito ACs. Para estabelecer esta relação de confiança, utilizando certificação cruzada, são necessários 56 certificados e 28 relações de confiança.

Com o aumento do número de ACs estabelecendo relações de confiança entre si, aumenta o consumo de tempo do administrador para verificar as políticas e práticas de cada uma das ACs.

Portanto, esta alternativa é uma ótima abordagem para estabelecer relações de confiança entre poucas ACs.

#### 3.5.2.2 Pontes

As Pontes de certificação digital foram criadas para resolver algumas lacunas da LCC e da certificação cruzada. Não é esperado que um usuário consiga gerenciar um número grande de relações de confiança, e os administradores precisam de um mecanismo mais eficiente para estabelecer relações de confiança com várias ACs. Para suprir estas demandas, as pontes agem como uma espécie de “mediador confiável”[8].

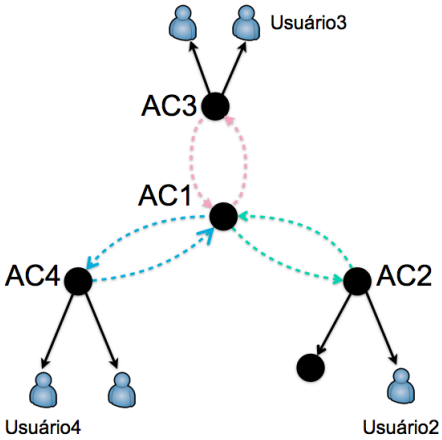


**Figura 3.14:** Ponte entre três entidades

Uma ponte é uma "AC especial", que estabelece relações de confiança entre diferentes ACs. Estas relações podem ser combinadas para formar "pontes confiáveis", que conectam os usuários de diferentes ICPs. As ACs que desejam criar relações de confiança entre si emitem um certificado para a AC Ponte, e esta emite outro certificado para cada uma das outras ACs. A AC que estabelece a relação de confiança com a AC Ponte é chamada de AC Principal [8]. Uma Ponte não pode emitir certificado para usuários, ela somente pode emitir certificado para outras ACs, e é ela que é responsável por avaliar a confiabilidade das ACs que querem estabelecer relações de confiança[8]. Sutilmente diferente da Autoridade Unificadora, a AC ponte não é utilizada como ponto de confiança. Todos os usuários consideram a Ponte como uma AC intermediária.

A figura 3.14 demonstra o esquema de Ponte. A AC1 é chamada de AC Ponte. As ACs 2, 3 e 4 emitiram um certificado para a AC1, e esta emitiu um certificado para cada uma das anteriores. Se o usuário 2, que possui como ponto de confiança a AC 2, for se comunicar com o usuário 3 (AC 3), o caminho de certificação do certificado do usuário 3 para o usuário 2 será: usuário 3 $\rightarrow$ AC3 $\rightarrow$ Ponte $\rightarrow$ AC2. Já para o usuário 3 será usuário 2 $\rightarrow$ AC2 $\rightarrow$ Ponte $\rightarrow$ AC3.

Como na certificação cruzada, adicionar ou remover relações de confiança com outras ACs é responsabilidade dos administradores. Se uma ICP desejar terminar a relação de confiança com as outras ACs, ela pode revogar o certificado emitido para a Ponte. Vale lembrar que uma vez revogado o certificado emitido de uma ICP para a ponte, é desfeita a relação de confiança com todas as ICPs conectada na Ponte.

Se uma AC Principal for comprometida, cabe ao administrador da Ponte revogar o certificado desta AC. Esta ação faz com que todas as outras ICPs ligadas a Ponte deixem de confiar na AC comprometida.

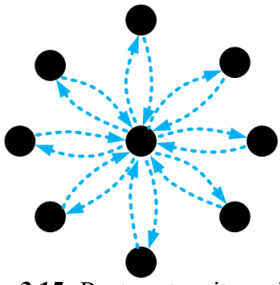

**Figura 3.15:** Ponte entre oito entidades

Se a AC Ponte for comprometida, ela notifica os administradores das ACs Principais, que revogam o certificado emitido para a AC Ponte. Dependendo do motivo de comprometimento da AC Ponte, ela pode emitir uma LCR revogando os certificados emitidos para as ACs Principais. Para reestabelecer as relações de confiança entre as ICPs, é necessário criar uma nova AC Ponte.

Quando há mais de duas ACs, montar o caminho de certificação em ponte é mais simples do que em certificação cruzada, pois, há somente um único caminho.

A grande vantagem de Pontes sobre Certificação Cruzada, é que ao estabelecer uma nova relação de confiança utilizando Ponte, somente é necessário criar uma relação de confiança e emitir dois novos certificados. A figura 3.15 apresenta o estabelecimento de confiança entre oito ACs utilizando uma AC Ponte. Esta é a mesma relação apresentada anteriormente, utilizando certificação cruzada. Para estabelecer esta relação de confiança, utilizando Ponte, são necessários apenas 18 certificados e 8 relações de confiança.

A principal limitação desta abordagem é a necessidade de criar uma AC para estabelecer as relações de confiança.

O gráfico 3.16 apresenta a comparação do número de certificados necessários para estabelecer relações de confiança utilizando certificação cruzada e pontes. No eixo Y estão representadas as quantidades de certificados necessárias para realizar certificação cruzada e ponte entre as quantidades de entidades descritas no eixo X. Note que, para poucas entidades, certificação cruzada demonstra ser mais simples, só que conforme o número de entidades aumenta, o aumento do número de certificados necessários aumenta exponencialmente. Enquanto que para pontes, este número aumenta linearmente.

## 3.6 CONCLUSÃO

Este capítulo apresentou alguns conceitos necessários para o entendimento deste trabalho, além de elucidar um pouco os principais conceitos de ICP. Ao final deste capítulo, foram apresentadas algumas alternativas

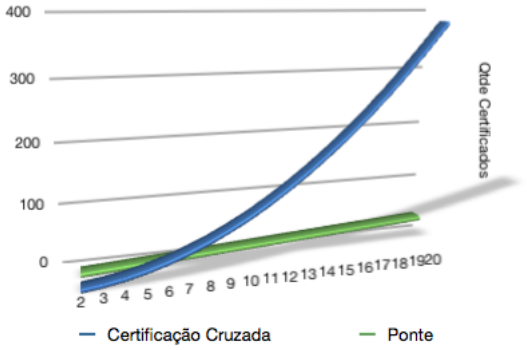


**Figura 3.16:** Gráfico comparativo entre certificação cruzada e bridge

para efetuar a comunicação entre diferentes ICPs, além de discutir os benefícios e limitações de cada uma das alternativas. Também foi apresentado um gráfico comparando o número de certificados necessários para integrar diferentes ICPs utilizando as abordagens de certificação cruzada e ponte. Através do gráfico, fica nítida a diferença entre as alternativas. A primeira é mais adequada para ambientes onde poucas ICPs irão se integrar. A segunda é melhor para ambientes onde várias ICPs vão se integrar, mas possui a limitação de necessitar da criação de uma AC para gerenciar as conexões. Na prática, talvez o maior empecilho seja a definição dos administradores da AC Ponte, os quais terão o poder de aprovar ou vetar a integração das ICPs.

# 4 POLÍTICAS DE CERTIFICAÇÃO

## 4.1 INTRODUÇÃO

Em segurança da computação, políticas estão relacionadas com o que pode ser feito, e quem pode fazê-lo [8, p. 25]. Autoridades Certificadoras possuem políticas que definem como elas atuam, e estas políticas influenciam diretamente no quanto confiamos nos certificados emitidos por ela. Em outras palavras, através das políticas de certificação um usuário (ou aplicação) pode determinar se a assinatura digital foi criada utilizando um certificado digital suficientemente seguro.

Os bancos emitem cartões de crédito somente para clientes que pagam suas contas. Eles determinam se o cliente paga as suas dívidas verificando o seu trabalho, salário, histórico de crédito, etc. Quanto mais confiante no cliente o banco estiver, maior será o limite disponibilizado. O emissor indica o nível de confiança, geralmente, através de um sistema de "cores", provendo cartões de crédito com diferentes classificações: "silver", "gold", "platinum" etc. O mesmo acontece com certificados digitais. Para o usuário verificar o nível de confiança associado a um certificado digital, é utilizado um mecanismo similar ao sistema de cores dos cartões de crédito. Em certificação digital, estas informações são chamadas de políticas de certificados.

Os cartões de crédito, além de possuírem a classificação de acordo com a confiança aplicada no cliente, possuem determinadas restrições. Alguns cartões somente podem ser utilizados em determinadas lojas, ou podem somente ser utilizados para comprar determinados tipos de bens ou serviços. Uma operadora de cartões de uma rede de lojas, pode restringir a utilização dos seus cartões a lojas participantes desta rede. Um cartão emitido por uma rede de postos de gasolina, pode restringir o cartão para ser utilizado somente para comprar gasolina, ou realizar reparos automotivos. Com este último não é possível comprar sapatos ou roupas. O mesmo acontece com certificados digitais. Uma aplicação precisa decidir se um certificado digital pode ser utilizado para determinados fins. Uma possível aplicação de políticas é determinar se um certificado pode ser utilizado para assinar contratos, ou se somente pode ser utilizado para assinar e-mails.

As políticas de certificado permitem ao emissor do certificado expressar o nível de confiança empregado no certificado, especificar restrições sobre o certificado digital, ou ainda definir um conjunto de aplicações possíveis para o certificado. A RFC3647 [45], apresenta um modelo, e instruções, de como escrever um documento de Políticas de Certificação. Embora alguns trabalhos, como [46], apontem deficiências na RFC3647, atualmente este é o principal documento utilizado para criar

documentos políticos em ICPs.

As próxima seções deste capítulo descrevem como estas políticas são implementadas em certificação digital.

## 4.2 EXTENSÕES DE POLÍTICAS

A necessidade de especificar políticas para determinar a confiabilidade e restrições de uso de um certificado é suprida através das extensões de políticas de certificação. Através destas extensões o emissor do certificado especifica qual a classificação de um certificado. Por exemplo, as extensões de políticas podem especificar que um determinado certificado digital pertence a um determinado grupo, com restrições e práticas de segurança, que suporta a assinatura de e-mails, porém os certificados deste grupo não podem ser utilizados para assinar contratos.

Através das extensões de políticas o emissor do certificado também pode descrever como foram tomadas as decisões ao emitir um determinado certificado, assegurando a cada um deles diferentes níveis de confiança. Dependendo do nível de confiança associado ao certificado, os usuários podem decidir se o certificado é compatível com suas aplicações.

Para definir estas "classes"de certificado, são utilizados dois tipos de documentos: Política de Certificado (PC) e Declaração de Práticas de Certificação (DPC). Estes documentos possuem o mesmo formato, porém possuem diferentes públicos e diferentes objetivos[8, p. 181]. A maioria dos usuários não buscam estes documentos diretamente, mas obtêm estas informações de políticas indiretamente, utilizando as extensões de certificação.

A inclusão destas políticas nos certificados digitais é feita através de duas extensões de certificado: *Certificate Policies* e *Policy Mappings*. Como estas extensões são muito flexíveis, podem ser necessárias outras extensões para impor limites. Estes limites são impostos pelas extensões *Policy Constraints* e *Inhibit anyPolicy*. Cada uma destas extensões será estudada detalhadamente nas próximas seções.

Estes três mecanismos (PC, DPC e extensões de políticas) são a base de políticas em ICP. Cada um destes satisfaz a necessidade dos diferentes públicos de uma ICP, e serão detalhados nas próximas seções.

## 4.3 POLÍTICAS DE CERTIFICADO

Uma Política de Certificado (PC) é um documento de alto-nível que descreve as políticas de segurança para emissão de certificados e manutenção do seu estado. Estas políticas de segurança descrevem a operação da AC, assim como a responsabilidade dos usuários por requisitar, usar e manusear os certificados e chaves. A PC assegura que estas políticas serão implementadas desde a geração do certificado até a expiração ou revogação. Ela não especifica como a política deve ser im-

plementada. Com a exclusão destes detalhes, uma PC torna-se bastante estável, e é razoável assumir que uma PC pode ser utilizada por 10 anos ou mais [8, p. 184].

O escopo de uma PC pode ser a operação de uma única AC e os seus mecanismos de suporte, ou de uma ICP inteira. Uma PC que descreve as operações apenas de uma AC é suficiente quando o ponto de confiança é o mesmo que emite os certificados dos usuários. Quando o ponto de confiança for diferente da AC que emite os certificados dos usuários, é necessário que a PC atue sobre toda a ICP. Caso contrário, não é possível assegurar o nível de segurança descrito na PC. Neste caso, a PC deve descrever as operações da AC Raiz e de todas as ACs que emitem certificados sobre esta política [8, p. 184].

A PC é utilizada por diferentes grupos de pessoas, por diferentes razões. Algumas delas:

- Desenvolvedores de aplicações - Analisam a PC para determinar se um certificado é apropriado para a sua aplicação;
- Auditores - Utilizam a PC para verificar se os procedimentos executados por uma determinada AC estão corretos;
- ACs de outras ICPS - Através da análise da PC é possível determinar a equivalência de políticas entre duas ICPs antes de realizarem uma integração;
- Autores de DPCs - Utilizam uma PC para guiar o desenvolvimento da DPC(ver seção 4.4) da AC que opera sobre a PC.

Toda PC possui um identificador único, chamado de Identificador de Objeto (OID). Os OIDs, por questões de padronização, são registrados por uma entidade específica, a Internet Assigned Numbers Authority (IANA). A numeração dos OIDs utiliza um sistema de numeração hierárquico. Somente pequenas alterações na PC podem ser feitas sem modificar o OID.

A PC geralmente é escrita baseando-se no formato padrão definido na RFC2527 [47], *Certificate Policy and Certification Practices Framework*. Esta norma é composta por oito seções principais, divididas em 185 tópicos. A aderência ao formato possui algumas vantagens:

- Como o formato é padronizado e bem definido, é mais difícil do escritor esquecer de definir algo importante;
- É muito difícil abranger os 185 tópicos sem um guia para definir os tópicos, e quais assuntos devem ser tratados em cada um deles;
- Ao estabelecer relações de confiança com outras ICPs, é mais fácil as políticas serem reconhecidas e compreendidas. A falta de compreensão neste caso pode levar ao impedimento do estabelecimento da relação de confiança;

- O mapeamento de políticas fica mais simples já que o documento está dividido com as mesmas seções.

As PCs são documentos que descrevem, em alto nível, os requisitos de determinadas "classes"de certificados. Outro documento importante relacionado com políticas de certificação são as DPCs, que especificam como as restrições impostas pela PC são implementadas. Este documento será descrito na próxima seção.

## 4.4 DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

O documento Declaração de Práticas de Certificação (DPC) é altamente detalhado e descreve como uma AC implementa uma PC específica. A DPC identifica a PC e especifica os mecanismos e procedimentos adotados para alcançar os requisitos definidos na PC [8, p. 185].

A principal diferença entre uma DPC e uma PC está no refinamento de detalhes da DPC. Enquanto a PC apenas especifica o que deve ser feito, a DPC especifica como deve ser feito. Por exemplo, se uma PC define: "Todos os requerentes de certificados devem ser autenticados pessoalmente por uma AR antes do certificado ser emitido", uma DPC que implemente esta PC, poderia definir: "Os requerentes somente receberão os seus certificados depois de se apresentarem pessoalmente a uma AR, com as seguintes credenciais: 1)Documento de identificação com foto, 2)Título de Eleitor, 3)Cópia do Cadastro de Pessoa Física (CPF)". Uma DPC inclui detalhes operacionais suficientes para demonstrar que a PC pode ser satisfeita pela combinação dos mecanismos e procedimentos [8, p. 185].

Cada DPC aplica-se a apenas uma AC. A DPC pode ser considerada como o manual de procedimentos gerais da AC. Partes específicas da DPC são extraídas para formar o Guia do Operador da AC, Manual da AR, ou outros documentos para funções específicas [8, p. 185]. Os auditores também fazem uso da DPC para validar a operação da AC, e verificar se os procedimentos satisfazem a PC. Segundo [8], uma DPC não precisa ser publicada, a combinação da PC com os resultados do processo de auditoria deveriam ser necessários para as partes externas.

As DPCs estão relacionadas com os OIDs de política através da PC que elas implementam [8, p. 185].

Uma PC pode ser implementada por diferentes DPCs, e uma DPC pode satisfazer os requisitos de mais de uma PC. As figuras 4.1 e 4.2 apresentam, respectivamente, estas condições.

Para escrever uma DPC, utiliza-se a mesma norma utilizada para escrever PCs, a RFC2527 [47] *Certificate Policy and Certification Practices Framework*. Os benefícios de utilizar esta norma foram especificados na seção 4.3. Além dos benefícios já apresentados, redigir ambos documentos (PC e DPC) baseando-se na RFC2527, facilita a comparação dos documentos, que podem ser comparados lado-a-lado. Esta comparação é

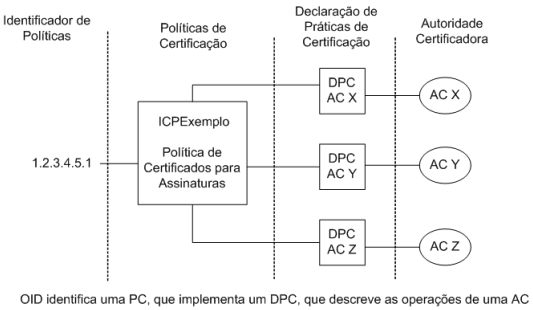


**Figura 4.1:** Implementação de uma PC por diferentes DPCs

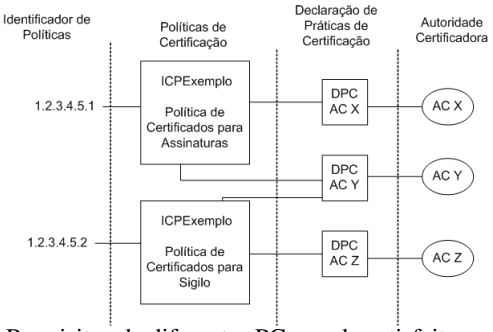


**Figura 4.2:** Requisitos de diferentes PCs sendo satisfeitos por uma DPC

necessária para assegurar que os procedimentos e mecanismos descritos na DPC implementam fielmente os requisitos da PC.

## 4.5 EXTENSÃO *CERTIFICATE POLICIES*

A extensão *Certificate Policies* é uma extensão que possui diferentes significados, dependendo do certificado que ela está associada. Se a extensão estiver associada a um certificado de Autoridade Certificadora, esta limita o conjunto de políticas permitidas em um caminho de certificação que contenha o certificado da AC. E quando ela estiver associada a um certificado de Usuário Final, indica sobre qual política(s) um certificado foi emitido. A política do certificado é identificada através de um OID, geralmente chamado de OID de política.

A extensão *Certificate Policies* lista uma ou mais políticas, identificadas através de um OID. Na lista de políticas especificadas na extensão *Certificate Policies*, não podem haver políticas repetidas (com mesmo OID). Nas figuras e exemplos utilizados neste trabalho, para maior clareza, ao invés de OIDs, serão utilizados nomes para as políticas, como *Prata*, *Ouro* e *Platina*.

A figura 4.3 apresenta um exemplo de uso da extensão *Certificate*

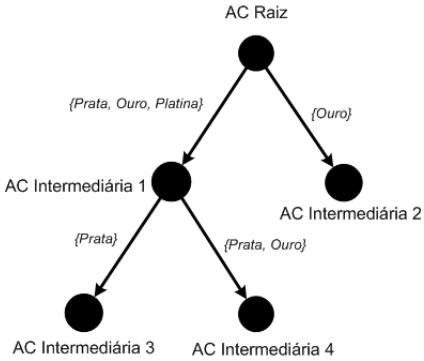


**Figura 4.3:** Políticas de Certificação - Exemplo 1

*Policies*. A AC Raiz definiu um conjunto de três políticas para a AC Intermediária 1. Ao definir este conjunto, a AC Raiz está afirmando que abaixo da AC Intermediária 1 somente podem ser emitidos certificados com as políticas Prata, Ouro e Platina. Já abaixo da AC Intermediária 2, podem ser emitidos certificados com a política Ouro. A AC Intermediária 1, emitiu um certificado para a AC Intermediária 3, com apenas uma política: Prata. Assim, a AC Intermediária 1 garante que a AC Intermediária 3 somente pode emitir certificados com a política Prata. A AC Intermediária 1 também emitiu um certificado para a AC Intermediária 4, com as políticas Prata e Ouro, assim A AC Intermediária 4 pode emitir certificados com

uma, outra, ou ambas políticas. Por último, somente a AC Intermediária 1 pode emitir certificados sobre a política Platina.

A figura 4.4 apresenta um exemplo de uso incorreto da extensão

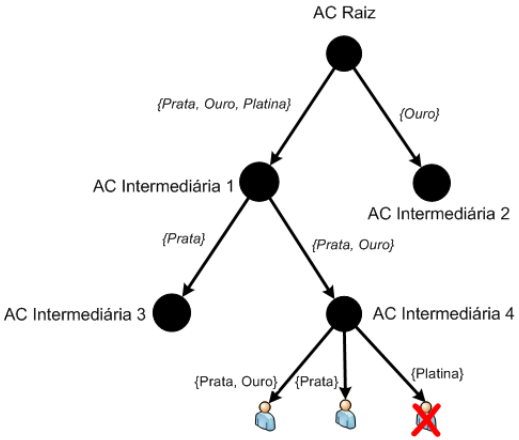


**Figura 4.4:** Políticas de Certificação - Exemplo 2

*Certificate Policies*. A AC Intermediária 4 emitiu três certificados de usuários finais. O primeiro com as políticas Prata e Ouro, o segundo somente com a política Prata, e o terceiro com a política Platina. Os dois primeiros certificados possuem políticas válidas, enquanto que o último não possui nenhuma política válida. Isto acontece porque a AC Intermediária 2 emitiu o certificado da AC Intermediária 4, especificando o conjunto de políticas Prata e Ouro, assim a AC Intermediária 2 somente pode emitir certificados com as políticas Prata ou Ouro. Nesta situação foi emitido um certificado com duas políticas, o que significa que ele pode ser utilizado para uma ou para outra política.

A figura 4.5 apresenta outro exemplo de uso incorreto da extensão *Certificate Policies*. A AC Raiz definiu um conjunto de três políticas para a AC Intermediária 1 (Prata, Ouro e Platina), e a mesma definiu um conjunto de políticas diferentes para a AC Intermediária 3 (Bronze e Diamante). Mesmo que a AC Intermediária 3 emita certificados seguindo as políticas definidas no seu certificado, as políticas destes certificados serão inválidas, pois a intersecção do conjunto das políticas dos certificados do caminho de certificação é vazio.

Na figura 4.6, a AC Intermediária 1 definiu um conjunto de políticas para a AC Intermediária 3, que inclui as políticas Prata, Ouro e Diamante. Os certificados emitidos pela AC Intermediária 3 com as duas primeiras políticas serão válidos, enquanto que os certificados emitidos com a última política (Diamante) serão inválidos.

Se a AC emissora não desejar limitar as políticas, ela pode utilizar um OID de política especial: 2.5.29.32.0, chamado de *Any policy*. Este

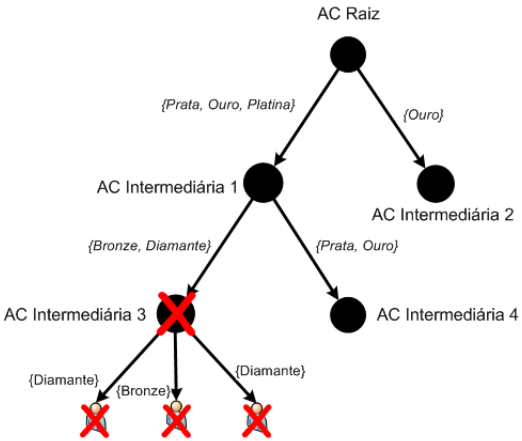


**Figura 4.5:** Políticas de Certificação - Exemplo 3

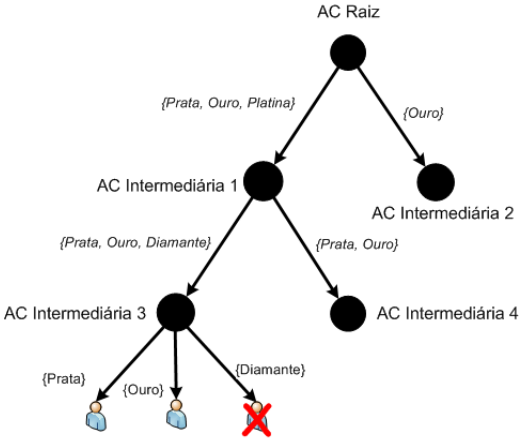


**Figura 4.6:** Políticas de Certificação - Exemplo 4

identificador serve para especificar que a AC pode emitir certificados sobre quaisquer políticas. O identificador especial *Any policy* (2.5.29.32.0) não deveria aparecer em certificados de usuário final.

A figura 4.7 mostra o exemplo de uso do identificador especial *Any policy*. A AC Raiz atribuiu o identificar *Any policy* para a AC Intermediária 1, e esta definiu um conjunto de políticas para a AC Intermediária 3, que inclui as políticas Prata, Ouro e Diamante. Agora, os certificados emitidos pela AC Intermediária 3 com as políticas Prata, Ouro ou Diamante serão válidos.

Cada política pode incluir um ou mais qualificadores de políticas, opcionais. Os qualificadores podem limitar uma política, porém espera-se

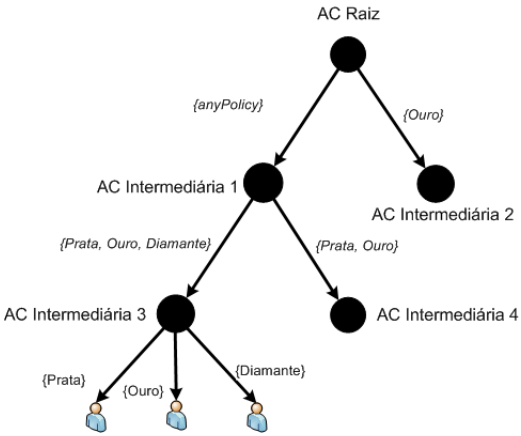


**Figura 4.7:** Políticas de Certificação - Exemplo 5

que eles não modifiquem as definições da políticas. Por exemplo, um OID de política pode indicar que o certificado pode ser utilizado para assinar mensagens de correio eletrônico, e o qualificador pode indicar que este certificado somente pode ser utilizado para troca de mensagens de correio eletrônico dentro da própria empresa.

Qualificadores de políticas impactam negativamente a interoperabilidade. Se uma política não for definida localmente, os usuários podem enfrentar dificuldades em utilizar certificados se as políticas não forem reconhecidas. Do ponto de vista técnico, o uso de qualificadores é fortemente desencorajado. Porém, os juristas adoram qualificadores. Os qualificadores oferecem uma maneira de embutir avisos, ou ponteiros para avisos. Exemplos destes avisos seriam termos de responsabilidades, avisos legais, notificações etc.

A RFC 5280 especifica e define a sintaxe de dois qualificadores: *CPS Pointer* e *User Notice*. O primeiro especifica um ponteiro para a Declaração de Práticas de Certificação, e o segundo especifica uma nota, que os usuários podem visualizar. Estes qualificadores serão detalhados a seguir. Embora mais qualificadores possam ser definidos, a RFC 5280 recomenda a utilização somente destes dois qualificadores.

### 4.5.1 CPS Pointer

O qualificador *CPS Pointer* contém um ponteiro para a DPC. Este ponteiro deve ser especificado no formato de uma URI, disponível na internet. Mais detalhes sobre a DPC podem ser encontrados na seção 4.4.

Se for utilizado o qualificador *CPS Pointer*, que aponta para a DPC da AC, a RFC5280 define que o processamento destas informações é um problema local, e não é tratado pela norma. Se for utilizado o qualificador *userNotice*, este apenas contém um texto curto que deve ser exibido ao

usuário quando o certificado for utilizado.

### 4.5.2 User Notice

O qualificador *User Notice* contém uma nota, que é apresentada ao usuário pela aplicação, quando o certificado digital for utilizado. O tamanho máximo desta nota é de 200 caracteres. Na RFC3280 (versão anterior da RFC 5280) era possível referenciar uma declaração emitida por uma determinada organização, porém a RFC 5280 recomenda fortemente não utilizar mais este qualificador desta maneira.

Por questões de interoperabilidade, a RFC 5280 recomenda que a extensão *Certificate Policies* somente seja definida utilizando o OID da política, sem utilizar qualificadores. Quando somente um OID não for suficiente, recomenda-se o uso apenas dos dois qualificadores definidos na RFC 5280 — *CPS Pointer* e *User Notice*.

Espera-se que as aplicações que necessitam de políticas específicas possuam uma lista com as políticas aceitáveis, e quando o certificado do usuário for utilizado, a aplicação deve comparar os OIDs das políticas do certificado do usuário com a lista de políticas aceitáveis.

A única obrigação que a RFC5280 faz em relação a extensão *Certificate Policies* é que se a extensão for marcada como crítica, as aplicações validadoras do caminho de certificação devem interpretar completamente a extensão (incluindo os qualificadores), e se não isto for possível, a aplicação deve considerar o certificado como inválido.

## 4.6 EXTENSÃO POLICY MAPPINGS

Quando duas ICPs operam sobre diferentes políticas, as aplicações não são capazes de reconhecer as políticas da outra ICP. Para a aplicação reconhecer a política da outra ICP, é necessário fazer um mapeamento entre as políticas compatíveis.

A extensão *Policy Mappings*, que é utilizada somente em certificados de AC, faz o mapeamento entre as políticas de diferentes domínios, como por exemplo entre duas ICPs.

A extensão *Policy Mappings* é composta por uma sequência de um ou mais pares de OIDs. Cada par contém um OID chamado de *issuerDomainPolicy*, e outro OID chamado de *subjectDomainPolicy*. Cada par indica que a AC considera a sua política *issuerDomainPolicy* equivalente a política *subjectDomainPolicy* da outra AC.

A extensão *Policy Mappings* não faz o mapeamento de qualificadores. Os qualificadores definidos na política *issuerDomainPolicy* devem conter o mesmo significado na política *subjectDomainPolicy*. Esta é uma justificativa adicional para não utilizar qualificadores de políticas.

A figura 4.8, adaptada de [8, p. 92], mostra o funcionamento da extensão Policy Mappings. A AC 1 possui as políticas Prata e Ouro, que significam, respectivamente, alto e baixo nível de segurança. A AC 2

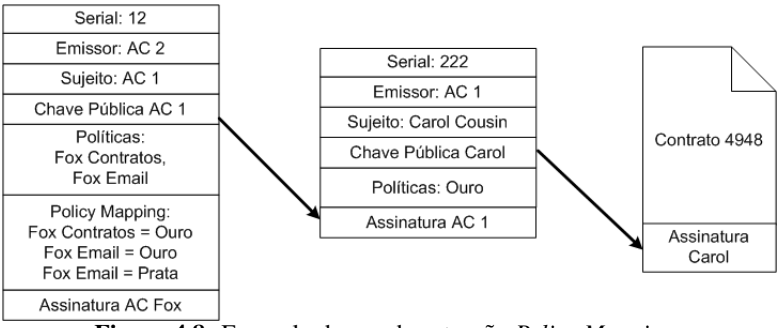


**Figura 4.8:** Exemplo de uso da extensão *Policy Mappings*

possui as políticas *Contratos* e *E-mail*, que expressam, respectivamente, certificados para assinatura de contratos e certificados de e-mail. A AC 2 faz o mapeamento das políticas Ouro e Prata para *E-mail*, e Ouro somente para *Contratos*. Assim, os certificados emitidos pela política Ouro podem ser utilizados como os certificados para assinatura de contratos da AC 2, e os certificados emitidos pela política Ouro ou Prata podem ser utilizados para validar e-mails assinados pelos usuários da AC 1.

O estabelecimento da correlação entre as políticas é uma tarefa complicada, e normalmente exige a intervenção dos administradores das entidades.

## 4.7 EXTENSÃO POLICY CONSTRAINTS

A extensão *Policy Constraints* é utilizada para impor limitações na validação do caminho de certificação. Esta extensão pode, durante o caminho de certificação, ignorar o mapeamento de políticas feito pela extensão *Policy Mappings* ou obrigar que todos os certificados do caminho de certificação possuam uma política definida. Estas restrições podem ser impostas aos certificados logo abaixo do certificado em que se encontra a extensão, ou podem ser impostas somente após um determinado número de certificados.

A extensão *Policy Constraints* é formada por dois campos: *inhibit policy mapping* e *require explicit policy*. Ambos os campos são formados por um contador. Este contador representa o número de certificados adicionais que podem aparecer no caminho de certificação antes das restrições serem aplicadas. O primeiro campo serve para inibir o mapeamento de políticas, e o segundo para obrigar que os certificados possuam uma política definida (a extensão *Certificate Policies* deve estar presente, e com um identificador de política válido).

A RFC5280 define que as aplicações devem interpretar o campo *require explicit policy*, porém não obriga as aplicações interpretarem o campo *inhibit policy mapping*. As aplicações que conseguem interpre-

tar o campo *inhibit policy mapping*, devem também conseguir interpretar a extensão *Policy Mappings*. Se a aplicação não conseguir interpretar o campo *inhibit policy mapping*, e a extensão *Policy Constraints* estiver marcada como crítica, a aplicação deve considerar o certificado como não válido.

De acordo com a RFC5280, esta extensão somente pode ser utilizada em certificados de AC, e deve ser marcada como crítica.

## 4.8 EXTENSÃO INHIBIT ANYPOLICY

A extensão *Inhibit anyPolicy* indica que o OID especial *any-policy* (2.5.29.32.0) não pode ser considerado como um identificador de política válido, exceto quanto aparecer em certificados de ACs intermediárias auto-emitido. Esta extensão é formada por um único campo, um contador que representa o número de certificados adicionais que podem aparecer no caminho de certificação antes da restrição ser aplicada.

Esta extensão somente pode estar associada a certificados emitidos para ACs, e deve ser marcada como crítica.

## 4.9 CONCLUSÃO

Neste capítulo foram apresentados os mecanismos utilizados para incorporar aspectos políticos nos certificados digitais, bem como a sua importância. Foram explicados detalhadamente cada um dos três mecanismos: a Política de Certificado, que define como devem ser os procedimentos e as restrições necessárias; a Declaração de Práticas de Certificação, que descreve como os procedimentos são implementados para alcançar os requisitos definidos na PC e; as Extensões de políticas, que são utilizadas para identificar as políticas relacionadas a um certificado digital.

# 5 INTEGRANDO ICPS

## 5.1 INTRODUÇÃO

É simples reconhecer e validar certificados e assinaturas digitais entre participantes que estão sob uma mesma ICP. Porém, entre diferentes ICPs, é necessário que a parte interessada confie direta ou indiretamente no certificado digital do usuário da primeira ICP.

Por exemplo, se duas organizações executam um trabalho colaborativamente, é necessário que as assinaturas digitais dos documentos eletrônicos veiculados entre as duas sejam reconhecidas mutuamente. Para isso, deverá haver algum mecanismo que permita aos usuários reconhecer e confiar nas assinaturas digitais de ambos os domínios. Outro exemplo, se a comunicação entre processos de diferentes equipamentos necessita ser feita de forma autêntica e inequívoca, surge a necessidade de haver alguma forma que permita identificar esses processos interdomínios. Assim, o software de gestão de ambos os dispositivos deve, de alguma forma, poder criar laços de confiança entre eles.

Nestes exemplos, se cada organização (ou dispositivo) contar com sua própria ICP, a confiança nas raízes de cada domínio precisa ser propagada aos diferentes domínios de interesse.

Existem na literatura propostas de mecanismos que permitem a integração de ICPs de grandes domínios. Entretanto, defendemos que tais mecanismos precisam ser melhor entendidos e aprimorados para que possam ser corretamente utilizados em larga escala.

Neste capítulo, na Seção 5.2 apresentam-se simulações que demonstram como os mecanismos de integração existentes na literatura, descritos na seção 3.5, funcionam. O objetivo destas simulações é elucidar melhor os métodos de integração, pois apesar da descrição relativamente detalhada por seus proponentes, alguns detalhes importantes normalmente passam desapercebidos, e implicam em dissonância entre diferentes aplicações, o que dificulta a correta integração de ICPs.

Em seguida, na Seção 5.3, a partir de uma análise dessas simulações, apresentam-se uma série de desafios que precisam ser devidamente tratados para que tais mecanismos possam ser empregados em larga escala. Após cada análise, são definidos alguns requisitos que precisam ser atendidos para viabilizar a integração de ICPs em larga escala.

Uma das maiores preocupações quanto a integração de ICPs é o correto tratamento das políticas de certificação. A questão a ser tratada é como mapear diferentes políticas entre um grande número de diferentes ICPs. A Seção 5.3 também apresenta recomendações que precisam ser adotadas para o uso correto das políticas.

Finalmente, na seção 5.4 realiza-se um comparativo entre os dois

principais métodos de integração de ICPs existentes na literatura, mas agora sob a luz das preocupações discutidas ao longo deste capítulo.

## 5.2 DESCRIÇÃO DOS TESTES DE INTEGRAÇÃO REALIZADOS

Na seção 3.5 foram descritos os principais mecanismos encontrados na literatura para a integração de ICPs, sendo eles: Certificação Cruzada, Ponte, Listas de Certificados Confiáveis Local, Autoridades de Confiança e AC Unificadora.

Nesta seção descrevem-se as dificuldades de implantação dessas soluções considerando as combinações de quatro ICPs primárias: Única AC, Malha, Hierárquica e Híbrida. Os métodos propostos por [29], [28] não foram avaliados, uma vez que ainda estão em estágio embrionário e carecem de algumas definições. É digno de mencionar que as estruturas supracitadas representam todas as hierarquias conhecidas de ICPs.

Os testes realizados foram divididos em três etapas. Na primeira, realizou-se combinações entre as estruturas primárias para avaliar situações de interesse práticos. Todas as possíveis combinações de duas, três, quatro e cinco estruturas foram verificadas. Como há somente quatro estruturas primárias, em alguns casos, elas foram repetidas. Todos os métodos de integração foram aplicados nas combinações anteriormente apresentadas. Nesta etapa constatou-se que uma vez detectada alguma dificuldade de integração relacionada com as características particulares de um método, esta se mantém independentemente da inclusão de novas estruturas ao domínio integrado. No entanto, caso o método de integração não apresente problemas na primeira vez, ou seja, na integração de duas ICPs, não foram detectados novos problemas relacionados ao processo de inclusão de outros ICPs à simulação. Nesses casos, constatou-se que somente havia um aumento no número de operações de integração. Foram então feitas algumas análises em relação a esse aumento de operações para cada um dos mecanismos de integração.

Após esta etapa, foi realizada a integração com oito ICPs, duas de cada ICP primária. Esta etapa teve por objetivo avaliar os impactos gerados pela integração de várias ICPs em um mesmo domínio. Todas as ICPs após integradas participaram de um mesmo domínio.

Na última fase, foi realizada a integração de cada uma das ICPs primárias com vários outros domínios (já integrados anteriormente), objetivando avaliar o desempenho na integração em larga escala. A ICP primárias utilizada, após as integrações participa de vários domínios ao mesmo tempo.

Estes foram os testes realizados para verificar os efeitos causados pela integração de ICPs. Todavia, durante o ciclo de vida de uma ICP, além das fases de integração, podem existir processos de desintegração dos domínios. Estes casos foram estudados através da repetição das integrações efetuadas anteriormente, geração de assinaturas digitais e autenticações e, posteriormente, a dissolução destes domínios.

As assinaturas digitais foram geradas considerando que algumas delas deveriam ter validade por pequenos períodos de tempo, e outras deveriam ser conservadas por um longo período de tempo. Dessas últimas, algumas ainda deveriam continuar válidas mesmo após a dissolução do domínio.

As assinaturas digitais foram feitas de acordo com três padrões: *XML Signature* (XMLDSig) [48], *XML Advanced Electronic Signature* (XAdES) [49] e *CMS Advanced Electronic Signature* (CAdES) [50]. A simulação da conservação destas assinaturas por longo prazo foi realizada através de Autoridades de Carimbo do Tempo, conforme descrito na RFC 3161 [43].

## 5.3 DIFICULDADES ENCONTRADAS

Nos testes realizados foram encontradas dificuldades relacionadas ao processo de integração, algumas manifestaram-se somente em determinados cenários simulados, outras apareceram devido as decisões tomadas pelos administradores das ICPs. Algumas já tinham sido descobertas e tratadas por outros mecanismos descritos na literatura, porém estes não foram consebidos para serem utilizados na integração de ICPs. A tabela 5.1 apresenta de forma resumida a influência causada por cada uma das dificuldades encontradas sobre os mecanismos estudado. Estas dificuldades são detalhadas nas próximas seções.

| Dificuldade | CC | Ponte | LCC | ACC | AU |
|---|---|---|---|---|---|
| Escolha da AC Principal | X | X | X | X | X |
| Caminho de Certificação | X | X | X | X | X |
| Políticas bem definidas | X | X | | | |
| Mapeamento de Políticas | | | X | X | X |
| Padrões de Assinatura | X | X | X | X | X |
| Compatibilidade de Algoritmos | X | X | X | X | X |
| Assinaturas a Longo Prazo | X | X | X | X | X |

**Tabela 5.1:** Dificuldades encontradas nos métodos de integração avaliados

### 5.3.1 Escolha da AC Principal

Para realizar a integração de ICPs é preciso escolher uma AC de cada ICP, denominada de AC Principal (ver seção 3.4.1). Não foram encontradas na literatura recomendações sobre como efetuar essa escolha e quais os impactos causados na integração.

Entretanto, este trabalho mostrou que não se pode escolher a AC Principal de forma aleatóri. Através dos testes realizadas, foi possível verificar que a escolha errônea da AC Principal pode comprometer a

verificação das assinaturas por entidades de outras ICPs participantes do domínio. A avaliação desta decisão deve ser cuidadosamente estudada pelo administrador da ICP antes de realizar a integração.

Quando a ICP utiliza estrutura hierárquica, a escolha de uma AC subordinada como AC Principal, pode fazer com que apenas um subconjunto de ACs participem do domínio de integração. A figura 5.1 apresenta a escolha de uma AC Principal subordinada. Nesta figura, a árvore (a) está

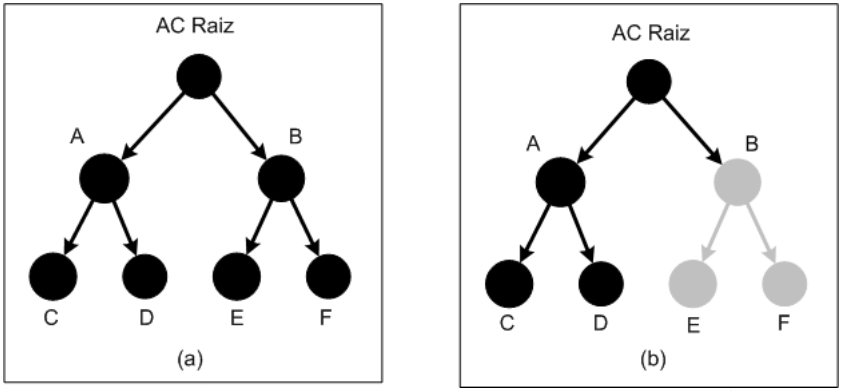


**Figura 5.1:** Influência da escolha da AC Principal - Arquitetura Hierárquica

representando toda a estrutura de uma ICP, que irá realizar a integração com outro domínio. Se o administrador escolher a AC Principal como "AC B", somente uma parte da árvore fará parte do domínio integrado. Esta parte é destacada na figura 5.1(b). Neste exemplo, as ACs A, C e D não serão integradas, e as assinaturas geradas abaixo destas ACs não serão validadas pelos integrantes dos outros domínios. Se esta ICP utilizar a AC Raiz como AC Principal, toda a árvore fará parte do domínio de integração. Este comportamento é observado em ICPs que utilizam o modelo hierárquico, pois, neste não há a emissão de certificados das ACs subordinadas para as ACs superiores.

Mesmo em ICPs que utilizam a arquitetura híbrida (ver seção 3.4.2.4), pode ocorrer o mesmo comportamento. Um exemplo é demonstrado na figura 5.2. Nessa ICP, se for escolhido a "AC C"como AC Principal, somente as ACs B e C participariam do domínio de integração. Este comportamento não acontece em ICPs que possuem arquitetura em malha, em que as ACs possuem certificação cruzada com todas as outras.

A definição de quais ACs farão parte do domínio de integração pode ser feita através da determinação do fecho transitivo inverso do vértice representante da AC Principal da relação que representa as entidades de uma ICP e seus certificados emitidos. Esta relação é definida como $DG(V, A)$, onde $V$ representa o conjunto dos vértices do dígrafo, e é definido como $V = \{e | e$ é uma Autoridade Certificadora pertencente à ICP$\}$, e $A$ representa o conjunto de arcos $x = (a, b), a$ e $b \in A$, de-

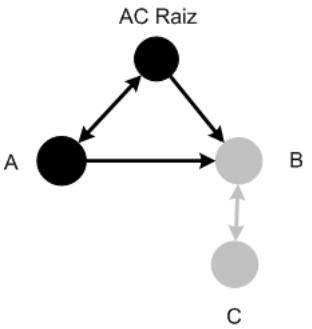


**Figura 5.2:** Influência da escolha da AC Principal - Arquitetura Híbrida

terminados segundo a relação $A = \{(a, b)|a$ emitiu um certificado para $b\}$.

Através da representação de uma ICP em forma de grafo também é possível verificar que nas ICPs que utilizam a arquitetura em malha, todas as ACs destas ICPs participam, pois estas são sempre representadas por dígrafos fortemente conexos[1].

### 5.3.2 Caminho de Certificação

A montagem e validação do caminho de certificação exige que o verificador possua acesso aos certificados que formam a cadeia de certificação. A obtenção destes certificados pode ser realizada por diferentes maneiras.

Uma ICP pode adotar diversos mecanismos para distribuir os certificados do caminho de certificação entre os seus participantes. Assim, quando os usuários forem verificar uma assinatura, eles possuirão os certificados necessários para montar o caminho de certificação. Estes certificados podem ser disponibilizados em algum sítio na Internet, através de um pacote de certificados disponibilizado aos participantes. Embora esta solução seja adotada por algumas ICPs, não existe um protocolo padrão difundido largamente para automatizar a busca de novas versões destes pacotes de certificados. Internamente as ICPs podem adotar mecanismos e normas próprias para os integrantes obterem estes certificados. Entretanto esta solução não é possível quando há integração com outras ICPs, visto que os integrantes dos novos domínios precisam conhecer estes mecanismos de obtenção dos certificados.

Além do método de distribuir os certificados do caminho de certificação, existem outras alternativas, como incluir o caminho de certificação na própria assinatura digital. De acordo com as principais normas e padrões mundiais, as assinaturas digitais podem conter re-

[1] Esses possuem a propriedade de que cada vértice pode ser alcançável partindo-se de qualquer outro vértice do grafo.

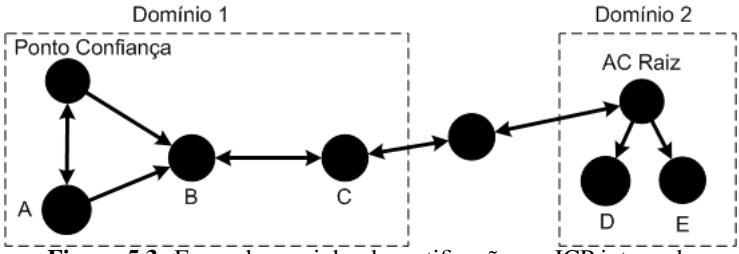


**Figura 5.3:** Exemplo caminho de certificação em ICP integrada

ferências para os certificados digitais do caminho de certificação, principalmente as assinaturas que precisam ser preservadas por longo prazo. Estas últimas costumam não ter apenas uma referência, mas uma cópia dos certificados utilizados. Isto é feito porque com o tempo estas referências podem passar a não ser mais válidas, e a verificação da assinatura, neste caso, não seria mais possível. Contudo, mesmo com esta solução, a verificação da assinatura por outros integrantes do domínio de integração pode ser comprometida. Isto ocorre devido ao fato que o caminho de certificação não inclui o certificado do ponto de confiança do emissor da assinatura (conforme descrito na seção 3.4.4). Sendo assim, faz-se necessário que os integrantes dos novos domínios de integração possuam em seus repositórios os certificados das âncoras de confiança de todas as ICPs.

Este problema pode ser agravado caso a AC Principal não seja ela mesma o ponto de confiança, pois as assinaturas digitais carregam somente os certificados entre o certificado do signatário e o seu ponto de confiança. A figura 5.3 apresenta um exemplo utilizando a arquitetura em malha. Se uma assinatura fosse feita por um usuário que teve o seu certificado emitido pela AC A, o caminho de certificação incluído em uma assinatura digital conteria somente o certificado da AC A. E, não incluiria os certificados necessários para um integrante de outra ICP validar a assinatura (que necessita dos certificados das ACs A, B e C, além do certificado da Ponte). Note que este problema não seria eliminado mesmo se a estrutura mostrada na figura 5.3 utilizasse a arquitetura de malha completa.

No exemplo anterior, se a integração fosse realizada utilizando certificação cruzada, o comportamento seria o mesmo.

A solução encontrada para este problema neste trabalho, é forçar o uso da extensão *Authority Information Access* (AIA) por todos os integrantes dos domínios (inclusive para os certificados utilizados para integrar as ICPs). Esta extensão aponta para um repositório contendo todos os certificados emitidos para o emissor do certificado que contém a extensão. Com esta extensão, os usuários de outras ICPs conseguem buscar automaticamente os certificados necessários para montar o caminho de certificação até o seu ponto de confiança, passando pela AC Princi-

pal e pelos certificados utilizados para fazer a integração (como o certificado cruzado, ou o certificado da ponte). Através do uso desta extensão, também é possível efetuar a validação de uma assinatura de um domínio em que a AC Principal não é o ponto de confiança.

### 5.3.3 Pontes de Pontes

Em larga escala, é factível imaginar que haverá a integração de domínios já integrados com outros domínios. Caso a integração de duas ICPs seja feita através de pontes, é possível que estas pontes se integrem a outras pontes, criando a integração de pontes de pontes.

A montagem do caminho de certificação nestes superdomínios se torna muito complicada sem o uso da extensão AIA(ver seção 3.4.5). A figura 5.4 demonstra um exemplo. Ela é composta por três domínios.

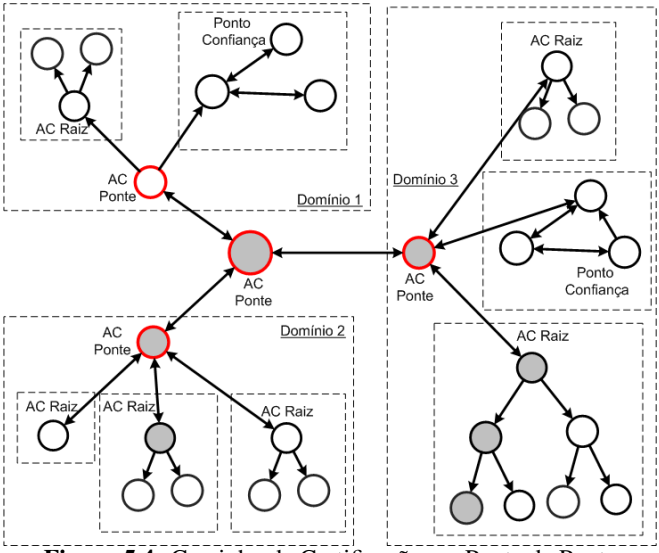


**Figura 5.4:** Caminho de Certificação em Ponte de Ponte

Cada um destes domínios é o resultado da integração de ICPs utilizando o método de Pontes. O domínio 1 é composto por duas ICPs, uma que utiliza o modelo hierárquico, e outra o de malha. O domínio 2 é composto pela integração de três ICPs, duas adotam o modelo hierárquico e noutra o modelo de Única AC. O domínio 3 é resultado da integração de três ICPs, duas hierárquicas e uma em malha. Estes três domínios, por sua vez, então integrados utilizando a técnica de Ponte, formando um "superdomínio".

Um integrante de determinado domínio, para validar assinaturas digitais realizadas em outros domínios, além dos certificados do seu domínio, precisa ter todos os certificados dos outros domínios. Caso ele não possua um dos certificados, pode não ser possível validar todas as

assinaturas do domínio. O uso da extensão AIA torna esta operação de obtenção de certificados transparente para o usuário.

A figura 5.4 destaca os certificados utilizados para um usuário de uma ICP do domínio 2 validar uma assinatura gerada em uma ICP do domínio 3. O usuário pertencente ao domínio 2, necessita possuir em seu repositório os certificados da sua ICP, da AC Ponte que integra o seu domínio, da AC Ponte que integra o superdomínio, da AC Ponte que integra o outro domínio, e das ACs da ICP em que a assinatura foi gerada. A cada nova composição de integração de ICPs, gera-se no mínimo um novo certificado a ser validado no caminho de certificação.

### 5.3.4 Necessidade de Políticas de Certificação bem definidas

A incorporação de informações de políticas em certificados digitais é realizada através da extensão *Certificate Policies* (CP). Essa extensão, quando presente em um certificado de Entidade Final, define sobre quais políticas o certificado foi emitido. Esta extensão é opcional segundo a RFC 5280 [3].

A ausência desta extensão em certificados que fazem parte de um domínio integrado pode dificultar a determinação da política que foi utilizada para emissão do certificado. Por exemplo, através das propriedades e extensões de um certificado definidas a partir da RFC 5280, não é possível saber se a chave privada está armazenada de forma segura em um hardware criptográfico ou na memória de um computador. Ou ainda, se a validação da identidade do usuário foi realizada de forma confiável.

Estas definições são essenciais para as aplicações identificarem quais certificados podem ser utilizados para realizar determinadas operações. Se determinada ICP adotar como regra que aplicações para assinatura de contratos devem certificar-se de que a chave privada dos signatários está protegida através de um dispositivo criptográfico, estas aplicações precisam conhecer quais políticas estabelecem como requisito o uso destes dispositivos. Assim, somente os certificados emitidos através destas políticas é que podem ser utilizados para assinar contratos. O comportamento pode ser observado na operação de validação da assinatura, quando a aplicação precisa determinar se a assinatura foi gerada por um certificado cuja chave privada correspondente está armazenada adequadamente.

A correta identificação destas e de outras características (que não podem ser identificadas através das propriedades de um certificado digital), está descrita no documento Políticas de Certificação (PC) e a forma como esta foi implementada está descrita no documento Declaração de Práticas de Certificação (DPC). A PC precisa estar devidamente referenciada nos certificados digitais. Isso é feito através da extensão *Certificate Policies*.

A validação de assinaturas geradas por outras ICPs de um mesmo domínio é realizada de acordo com as regras da ICP em que a assinatura

está sendo validada. Como geralmente as políticas entre uma ICP e outra são diferentes, é necessário realizar o mapeamento de políticas (conforme descrito no capítulo 4). Se as políticas em uma das ICPs pertencentes ao domínio não estiverem corretamente definidas, o mapeamento é prejudicado, podendo resultar na invalidação de assinaturas.

Algumas ICPs podem utilizar qualificadores de políticas, que dificultam o mapeamento de políticas, conforme explicado na seção 4.6. Alguns qualificadores também não possuem uma representação formal, como por exemplo o qualificador *CPSPointer*4.5.1, que indica aonde encontrar uma determinada DPC, documento normalmente escrito em linguagem humana.

A avaliação da compatibilidade entre políticas geralmente é feita de forma manual, pois os documentos que determinam os requisitos e formas de operação das ACs são escritos em linguagem natural. Isso dificulta o reconhecimento e interpretação de forma automática por máquinas. No entanto, na literatura podem ser encontrados trabalhos relacionados a este tópico, como [51], [52] e [53] que propõem formas de interpretar estes documentos, e gerar relações de equivalência entre eles, possibilitando a automatização de parte do processo de avaliação das políticas. A avaliação não pode ser totalmente automatizada uma vez que algumas partes necessitam de iteração humana. Além disso, nas partes que podem ser automatizadas nem sempre se consegue resultados com grande precisão.

O autor deste trabalho acredita que novos estudos, no futuro, possibilitarão a automatização do processo de análise, avaliação e comparação de políticas, levando à automatização do processo de mapeamento entre elas. Outra forma, talvez um pouco mais simples de implementar, seria a utilização de formatos de representação de políticas de fácil interpretação por computadores, como XML [54]. Entretanto, esta limita a capacidade de expressão que os atuais documentos de políticas possuem.

### 5.3.5 Mapeamento de Políticas em LCC e Autoridades de Confiança

As técnicas de integração de ICPs que se baseiam no uso de mecanismos externos (ver seção 3.5.1), como LCC e Autoridades de Confiança, não apresentam, em suas propostas, mecanismos adequados para realizar o mapeamento de políticas entre diferentes domínios. Esta é uma característica intrínseca dessas abordagens. Isso se deve ao fato que o mapeamento de políticas, feito através da extensão *Certificate Policies*, necessita da emissão de novos certificados, característica esta que identifica um mecanismo de integração através de domínios.

Em LCC, a integração é realizada apenas adicionando o certificado da AC Principal na lista de certificados confiáveis do usuário (mais detalhes na seção 3.5.1.1). Consequentemente, as assinaturas feitas nos domínios externos, ao serem validadas, apresentarão políticas pertencentes ao conjunto de políticas do domínio externo, pois não existe o mape-

amento das políticas externas para as internas. Isto pode causar o não reconhecimento das políticas externas pelas aplicações internas, resultando em resultados equivocados na verificação de assinaturas externas.

O mesmo efeito pode ser observado com a técnica de integração através de Autoridades de Confiança.

Uma forma de suprir esta dificuldade é emitir um certificado do primeiro domínio para o segundo domínio, e este certificado ser adicionado como confiável na LCC (ou ser adicionado à lista de certificados confiáveis emitido pela Autoridade de Confiança). Entretanto, se esta solução não for adotada por ambas as ICPs, não haverá o reconhecimento mútuo das assinaturas. Ao serem emitidos certificados da primeira para a segunda, e vice-versa, caracteriza-se uma certificação cruzada. Esta abordagem, conforme demonstrado na seção 3.5.2.1, não necessita de uma LCC, o que implica na inutilização da solução inicialmente escolhida.

### 5.3.6 Padrões de Assinatura

A manutenção de padrões "internos"pode ser simples internamente, porém na integração de ICPs, a verificação das assinaturas precisa ser interoperável. Recomenda-se a não utilização de atributos e extensões proprietárias e a utilização de algoritmos "puros"para validar assinaturas, sem o uso de políticas de assinatura. Cada ICP tem o seu procedimento de validação, e é necessário que as assinaturas contemplem os campos necessários para que estes algoritmos funcionem. Os algoritmos precisam funcionar considerando que vão ser realizadas validações de outras ICPs, e se o algoritmo depender de alguma característica não muito difundida, poderá haver problemas para validar as assinaturas.

Em 28 de Novembro de 2008, a Comissão Européia adotou um plano de ação para facilitar a integração de serviços que utilizam assinaturas digitais no mercado comum [55]. A partir deste plano, através de estudos realizados, vários padrões foram propostos pelo *European Telecommunications Standards Institute* (ETSI), como o *XML Signature* (XMLDSig) [48], *XML Advanced Electronic Signature* (XAdES) [49], *CMS Advanced Electronic Signature* (CAdES) [50], e o *PDF Advanced Electronic Signature* (PAdES) [56, 57, 58, 59, 60]. Devido a sua flexibilidade, estes padrões podem ser adotados por vários países. Em 22 de Dezembro de 2009, a Comissão Européia emitiu um mandato de padronização de assinaturas digitais [61], em que elege os formatos criados pelo ETSI como padrões para toda a união européia.

Embora estes padrões estejam sendo empregados em diversas ICPs, estes não são totalmente interoperáveis. Nem sempre há uma total correspondência entre os atributos e operações que estes padrões possibilitam, dificultando, em alguns casos, a conversão automatizada(sem conflitos) entre eles.

### 5.3.7 Compatibilidade entre algoritmos aceitos por aplicações

Nas simulações realizadas foram utilizados diferentes algoritmos para as chaves privadas das entidades. A probabilidade de haver tal diferença na integração de diferentes dispositivos é alta. As simulações demonstraram que a escolha dos algoritmos de chaves privadas, mesmo que obedecendo a determinados padrões, não garantiram a inter-operabilidade entre as aplicações. Isto aconteceu devido ao fato que algumas aplicações apresentam um conjunto de algoritmos determinados como recomendáveis por uma determinada norma, e outras aplicações implementam outro conjunto de algoritmos, determinado como recomendável por outra organização ou norma.

A dificuldade encontrada foi maior com algoritmos de Curvas Elípticas, os quais possuem mais parâmetros, criando muitas variações de entradas e especificações, dificultando a padronização de curvas a serem utilizadas. As tabelas 2.4 e 2.5, da seção 2.5, apresentam um levantamento sobre as curvas recomendadas pelas principais normas vigentes. Através deste levantamento, pode-se observar que o uso das curvas secp256r1 e secp384r1 é que traz a maior compatibilidade. Estes resultados foram observados durante as simulações. A biblioteca de criptografia CryptoAPI [20], presente no navegador *Internet Explorer*, implementa os algoritmos recomendados pela Suite B da NSA, já a biblioteca NSS [19], presente no navegador Mozilla Firefox, implementa os algoritmos recomendados pelo NIST.

### 5.3.8 Preservação de Assinaturas a Longo Prazo

A validade dos documentos digitais pode ser dividida em curto prazo e longo prazo. Do ponto de vista de integração de ICPs, as assinaturas de curto prazo não apresentam dificuldades relativas a sua expiração, pois a data de expiração destas assinaturas é menor que a data de expiração dos certificados presentes no caminho de certificação. Porém, as assinaturas de longo prazo podem ultrapassar a validade do certificado utilizado para fazer a integração, criando algumas dificuldades para manter estas assinaturas válidas após a expiração deste certificado.

Por exemplo, um documento que identifica atributos de um determinado produto (como data de compra, valor etc) que foi expedido por uma determinada ICP participante de um domínio integrado, necessita ser válido durante todo o ciclo de vida deste produto, e não somente enquanto esta ICP estiver participando do domínio.

Enquanto as ICPs estiverem participando do mesmo domínio, a validação da assinatura é feita como explicado na seção 3.4.7. Entretanto, quando domínios são integrados, há a necessidade de validar assinaturas geradas por outras ICPs pertencentes ao novo domínio. A diferença deste processo, após a integração de domínios, é demonstrada na figura 5.5, que destaca os certificados utilizados por um usuário para validar a assinatura feita por um usuário pertencente a outra ICP. Além da validação da assi-

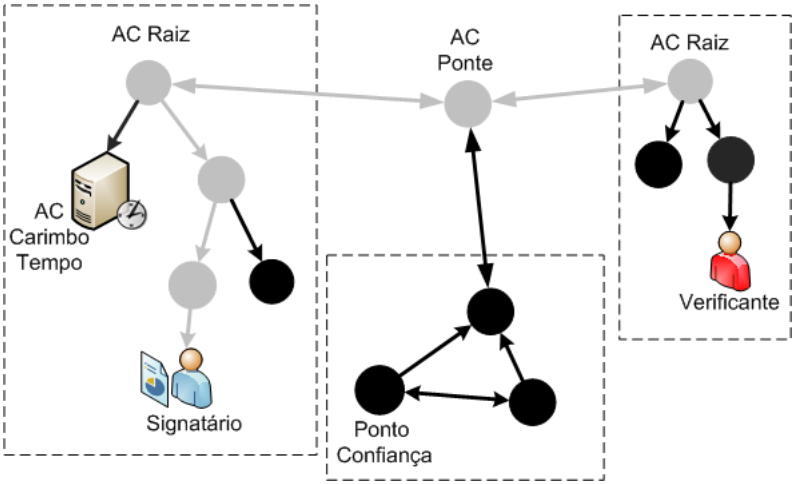


**Figura 5.5:** Caminho de certificação em domínios - Assinatura Digital

natura, é necessário validar os carimbos do tempo anexos as assinaturas. A figura 5.6 destaca os certificados utilizados para verificar carimbos emi-

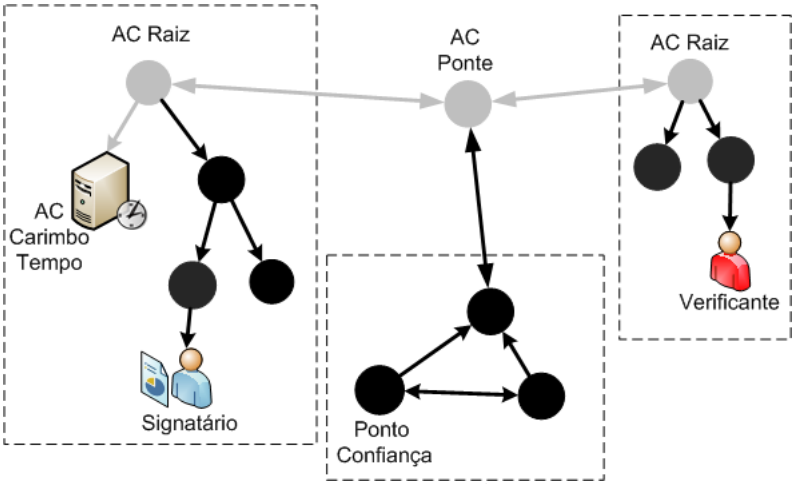


**Figura 5.6:** Caminho certificação em domínios - Carimbo do Tempo

tidos por Autoridades de Carimbo de Tempo que não pertencem a mesma ICP do verificador. A verificação da assinatura (e consequentemente do carimbo do tempo), é simples enquanto os domínios estão integrados, todavia, quando há a saída de um dos membros do domínio, a validação de carimbos do tempo é influenciada. Os carimbos do tempo emitidos por uma Autoridade de Carimbo do Tempo vinculada a uma AC Principal que

não pertence mais ao domínio não poderão ser mais verificados, comprometendo o processo de verificação da validade da assinatura digital por outros membros. Isto ocorre devido ao fato que os carimbos do tempo são validados utilizando a data atual. Vale ressaltar que a verificação da validade desta assinatura dentro da ICP em que foi gerada, em nada é afetada com a saída de membros, ou a dissolução do domínio.

Portanto, mesmo com a conservação da assinatura digital sendo efetuada por uma Autoridade de Carimbo do Tempo, após a ICP que conserva a validade da assinatura deixar de participar do domínio, a validade destes documentos é perdida (se o certificado do signatário já expirou).

O problema de revogação do certificado de uma Autoridade Certificadora superior a Autoridade de Carimbo de Tempo, não é tratado na RFC3161 [43]. Internamente nas ICPs, este problema pode ser omitido, se a emissão dos certificados das Autoridades de Carimbo de Tempo for feita pelo ponto de confiança.

Na literatura não foram encontradas outras soluções para este problema aplicáveis para domínios integrados. Foram então elaboradas cinco abordagens para contornar esta dificuldade, que serão detalhadas nas próximas seções.

#### 5.3.8.1 Abordagem 1

A primeira abordagem encontrada para solucionar o problema da conservação das assinaturas geradas dentro de um domínio, é que cada parte interessada na validade de determinada assinatura conserve a assinatura. Assim, quando houver o rompimento da participação de uma ICP no domínio, os documentos poderão continuar a ser validados pelas outras ICPs do domínio.

A principal desvantagem desta abordagem é que a quantidade de esforço dispendido para conservar um determinado documento, aumenta de acordo com o número de ICPs participantes do domínio. Se um determinado documento precisa ser validado por quatro ICPs pertencentes a um domínio, o trabalho será quatro vezes maior do que conservar apenas uma assinatura. Este custo se torna maior ainda em assinaturas de longo prazo, pois todas as vezes que for necessário carimbar novamente um documento, serão necessários cinco novos carimbos (um pela ICP que emitiu o documento, e outros quatro pelas ICPs que precisam validar este documento).

A figura 5.7 apresenta um exemplo da aplicação da abordagem proposta. Na figura estão destacadas as posições de três autoridades de carimbo do tempo, presentes em um domínio fictício. Através desta abordagem, todos os documentos que forem gerados por uma ICP, e que precisam ser validados pelas outras duas ICPs, necessitam ser carimbados por todas as três Autoridades de Carimbo do Tempo. Estas, representadas por ícones de computadores com relógios na figura 5.7.

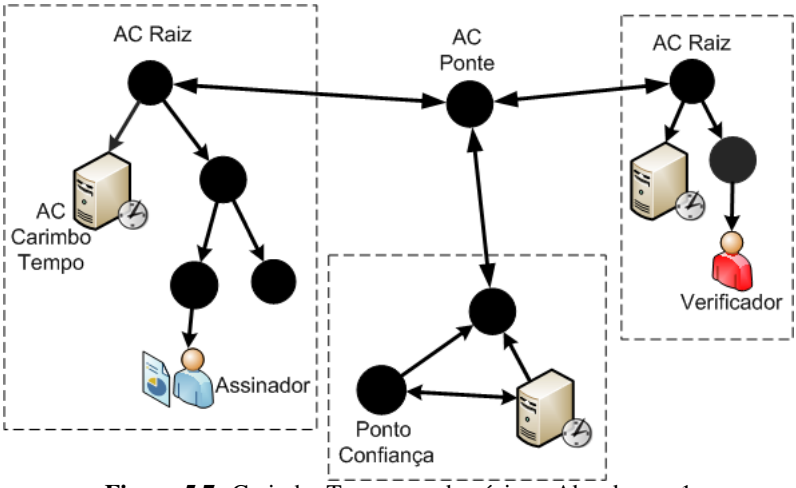


**Figura 5.7:** Carimbo Tempo em domínios - Abordagem 1

#### 5.3.8.2 Abordagem 2

Outra abordagem que pode ser considerada para resolver a preservação de documentos a longo prazo na integração de ICPs que utilizam o mecanismo de ponte, é a criação de uma nova Autoridade de Carimbo do Tempo, que estaria vinculado com a AC Ponte.

Esta carimbadora seria utilizada apenas para preservar os documentos que foram emitidos por uma ICP, e precisam ser validados por outras ICPs. Os documentos que transitarem somente internamente a ICP, poderiam ter a sua validade conservada pela suas próprias Autoridades de Carimbo do Tempo.

Ao desfazer o relacionamento de confiança entre uma determinada ICP e a Ponte, as outras ICPs podem continuar a validar as assinaturas dos documentos, baseados nos carimbos do tempo emitidos pela carimbadora vinculada à AC Ponte, pois esta continua a pertencer ao domínio. Após a validação da data do carimbo do tempo, a montagem do caminho de certificação a ser validado, é feita com base na data em que a assinatura foi feita, no qual aquela ICP ainda pertencia ao domínio, e os certificados de integração ainda não tinham sido revogados.

Durante a validação de uma assinatura utilizando esta alternativa, primeiramente é montado o caminho de certificação da Autoridade de Carimbo do Tempo, a que está associada à AC Ponte, conforme demonstrado na figura 5.8. Os certificados deste caminho são montados com base na data atual. Após a validação do carimbo do tempo, é montado o caminho de certificação da assinatura, com base na data em que a assinatura foi gerada, isto é, o *status* dos certificados (revogado ou não) é considerado utilizando-se a data do passado. Como na data em que a assinatura

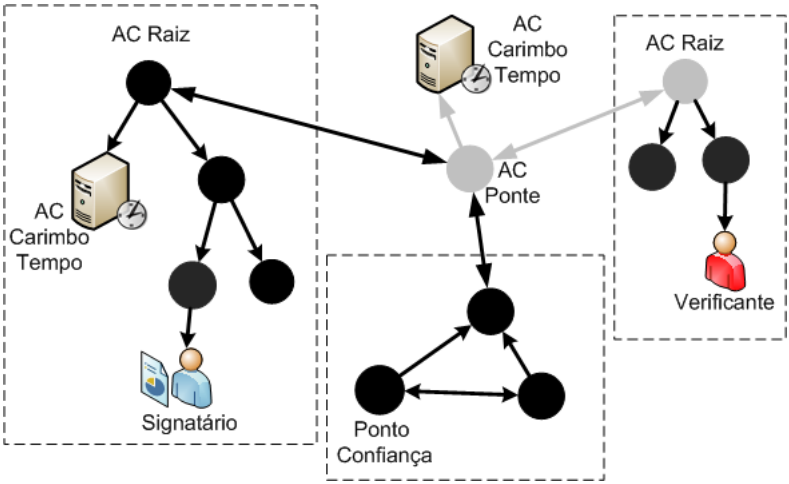


**Figura 5.8:** Carimbo Tempo em domínios - Abordagem 2

foi realizada, o certificado utilizado para fazer a integração da ICP com o domínio ainda não tinha sido revogado, a assinatura pode ser validada.

Esta abordagem pode ser expandida, e prover outros serviços para o domínio integrado. Este trabalho sugere que estes novos serviços devem ser fornecidos através de entidades criadas especificamente para esta finalidade.

#### 5.3.8.3 Abordagem 3

Uma outra abordagem, também atrelada ao uso de pontes, seria a emissão de certificados para as Autoridades de Carimbo de Tempo pela AC Ponte. Assim, todas as carimbadoras passariam a gerar carimbos que podem ser validados pelos outros integrantes do domínio, independentemente da existência de um certificado válido entre a AC Principal e a AC Ponte.

Desta maneira, todas as assinaturas carimbadas por alguma das autoridades de carimbo do tempo pertencentes ao domínio, poderiam ser validadas pelas outras ICPs pertencentes ao domínio. Um exemplo desta situação é apresentado na figura 5.9, em que a AC Ponte emitiu três certificados, um para cada uma das Autoridades de Carimbo de Tempo do domínio. Um documento, assinado por um usuário de uma ICP, e carimbado pela Autoridade de Carimbo de Tempo daquela respectiva ICP, ao ser validado por um usuário pertencente a outra ICP, será feito da seguinte maneira: 1) O carimbo do carimbo do tempo será validado, utilizando o caminho: AC Carimbo Tempo, AC Ponte, AC Principal do usuário verificador, conforme destacado na figura 5.10; 2) A assinatura será validada de acordo com o caminho de certificação existente na data em que a assi-

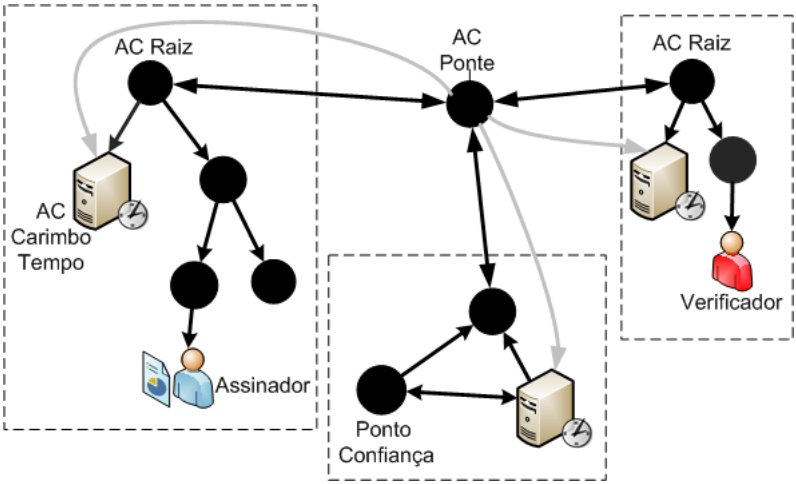


**Figura 5.9:** Carimbo Tempo em domínios - Abordagem 3

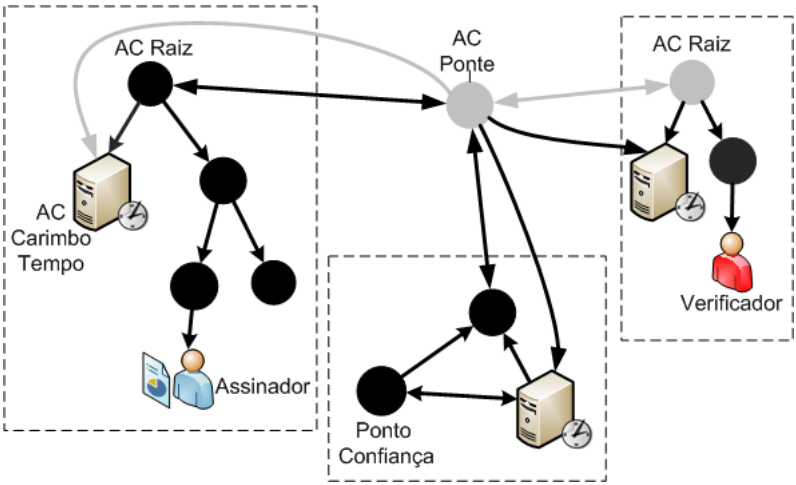


**Figura 5.10:** Carimbo Tempo em domínios - Alt. 3 - Caminho de certificação

natura foi gerada, passando pelo pela AC Principal do signatário (que na data da assinatura era válida), AC Ponte, e AC Principal do usuário que está validando a assinatura.

#### 5.3.8.4 Abordagem 4

Uma das desvantagens da primeira técnica apresentada, é a multiplicação polinomial da quantidade de carimbos necessários para manter uma assinatura digital válida por longo prazo. Esta quantidade de

carimbos pode ser amenizada reduzindo o número de carimbos emitidos.

Uma abordagem, para diminuir o número total de carimbos, é reduzir a quantidade de documentos a serem carimbados. Isto pode ser feito através da filtragem dos documentos a serem preservados.

Como o problema inicial, sobre a preservação de documentos a longo prazo, acontece somente após a saída de algum dos membros do domínio, pode-se postergar a manutenção destas assinaturas digitais, até o momento da saída de algum membro. Sendo assim, somente serão carimbados os documentos válidos, e emitidos pela ICP que está saindo, no momento da sua saída. Obtem-se desta maneira uma grande redução no número de documentos a serem carimbados. Serão necessários $n \times x$ carimbos, com $n$ representando o número de documentos que foram emitidos pela ICP que está saindo, e necessitam ser conservados por longo prazo, e $x$ representa o número de Autoridades de Carimbo de Tempo que pertencem as diversas ICPs do domínio.

Uma outra otimização possível, é que a responsabilidade de conservação da validade destas assinaturas seja transferida para outra ICP, assim, após a saída de uma ICP, serão necessários emitir apenas $n$ carimbos, com $n$ representando o número de documentos que foram emitidos por aquela ICP, e necessitam ser conservados a longo prazo.

Porém, esta abordagem pode gerar dificuldades se a saída de algum dos membros do domínio não for prevista.

#### 5.3.8.5 Abordagem 5

O autor deste trabalho acredita que a solução ideal, seria que ao aplicar um carimbo do tempo em uma assinatura de um determinado domínio, este carimbo fosse automaticamente validado pelos demais integrantes do domínio. Para isto ser possível, é necessário alguma forma de validação universal, em que qualquer domínio possa validar os carimbos emitidos por uma Autoridade de Carimbo do Tempo.

A solução mais próxima da solução ideal identificada neste trabalho, foi a criação de uma Autoridade Múltipla de Carimbo do Tempo (AMCT). Esta atua da mesma forma que uma Autoridade de Carimbo do Tempo, mas, o carimbo gerado possui uma forma diferente de ser identificado.

A Autoridade de Carimbo do Tempo identifica o carimbo emitido através de um atributo chamado *ESSCertID*, composto por três atributos: Um resumo criptográfico do certificado da ACT, O nome do emissor do certificado da ACT, e o número serial do certificado da ACT. Os dois últimos atributos são opcionais. Desta forma, um carimbo do tempo fica vinculado ao certificado de uma determinada ACT. Este atributo também pode conter vários certificados. Se assim ocorrer, o primeiro certificado é identificado como o certificado da ACT, e se a assinatura do carimbo do tempo não puder ser verificada com este certificado, ela é considerada inválida.

Este trabalho propõe que isto seja modificado, criando uma nova Autoridade Certificado chamada de AMCT. Nesta, o atributo que identifica a AC emissora do carimbo de tempo é modificado para identificar a AC apenas através do resumo criptográfico de sua chave pública.

Com isto, consegue-se criar diversas AMCT, em diferentes domínios. E, se estas contarem com a mesma chave pública, um carimbo gerado por qualquer uma das AMCTs do domínio, poderá ser validada por qualquer outra ICP do domínio, mesmo após a saída de uma delas.

Esta nova autoridade traz como desvantagem a necessidade de compartilhar uma chave privada entre várias ICPs. Entretanto, com a criação de um algoritmo que permita criar várias chaves privadas e apenas uma chave pública, será possível que cada AMCT de cada domínio possua uma chave diferente.

## 5.4 CERTIFICAÇÃO CRUZADA X PONTE

Os benefícios e limitações das duas principais técnicas de integração: Certificação Cruzada e Ponte, já foram descritos nas seções 3.5.2.1 e 3.5.2.2, respectivamente. Estas seções apresentam uma análise destas técnicas, sobre o foco da integração de grandes infraestruturas, geralmente organizacionais, governamentais etc. Ao considerar técnicas de integração, sobre a luz da integração em massa de diversos dispositivos, alguns outros princípios precisam ser considerados.

O primeiro, é a criação de uma nova AC caso for utilizado a técnica de integração de Pontes. Como decidir qual dispositivo irá gerenciar a Ponte? Na integração de infra-estruturas organizacionais, isto é feito através de acordos e regras estabelecidas, geralmente, entre as partes integrantes. A utilização de uma AC Ponte, disponível permanentemente, não é um problema para estes casos. Porém, quando há a necessidade de realizar a integração entre dispositivos, a maioria destes não ficam em estado operacional sem interrupções. Geralmente eles são utilizados por um determinado período, e após cumprirem a sua função são desligados, ou mudam para um estado de economia de energia, em que quase todas as funcionalidades são desativadas.

A melhor solução encontrada por este trabalho, foi limitar o uso de Pontes somente quando o número de dispositivos a ser integrados for grande, ou, por outros fatores, for necessário a utilização de uma AC Ponte para integrar os dispositivos. Nos outros casos, é recomendável dar preferência à Certificação Cruzada.

A certificação cruzada tem como principal vantagem que se um dos dispositivos for desligado (ou hibernar), não irá comprometer a integração do domínio. Ao utilizar esta abordagem, também podem ser criados diferentes caminhos de certificação para chegar a um mesmo ponto, possibilitando criar caminhos alternativos entre dois pontos da estrutura.

A utilização do método de integração por pontes é recomendável caso seja criado um dispositivo específico para realizar a integração de

dispositivos, semelhante ao que acontece com as conexões de rede, em que há dispositivos específicos para integrar os cabos de rede. Estes dispositivos poderia ser colocado em determinadas áreas, a fim de realizar a integração de múltiplos dispositivos, e gerir múltiplas pontes. Um exemplo prático seria a utilização de apenas um dispositivo desse dentro de uma casa, e todos os dispositivos eletrônicos fariam as suas integrações através deste. A maior dificuldade de criação de um dispositivo como este é a quantidade de padrões de comunicação que este necessita atender, a fim de possibilitar que vários dispositivos se conectem com ele. Além, é claro, de realizar a conversão entre diferentes protocolos e interfaces de comunicação.

Outro ponto a ser observado é o tempo de duração dos domínios integrados de dispositivos. Enquanto em organizações, geralmente, este período é longo, compreendendo anos, e com poucas modificações na infraestrutura, em dispositivos estas comunicações tendem a ser mais dinâmicas, com a criação e dissolução de vários domínios durante o seu ciclo de vida. Estes, também tendem a participar de vários domínios ao mesmo tempo, ao contrário das integrações organizacionais, gerando a necessidade de avaliação dos efeitos causados pela dissolução do domínio.

Na integração em massa de diferentes dispositivos, podem existir as mais variadas estruturas de ICPs, e para a comunicação entre elas ser possível, é necessário determinar mecanismos padronizados para executar todas as operações dentro do domínio. Nos domínios organizacionais, alguns detalhes não necessitam ser padronizados, ou passíveis de automatização, e podem ser supridos através de acordos ou termos políticos. Isto, atualmente, pode ser observado na padronização da geração e verificação de assinaturas digitais, em que diferentes ICPs adotam diferentes mecanismos, que nem sempre são compatíveis.

Através deste trabalho foi possível identificar que há falta de padronização em alguns aspectos da integração de ICPs, deixando os domínios heterogêneos, o que agrava muito a dificuldade de integrá-los.

## 5.5 CONCLUSÃO

Neste capítulo, foram discutidos os métodos mais utilizados para realizar a integração de ICPs, e foram detalhados os testes realizados. Estes, serviram para elucidar alguns aspectos destes métodos, e também serviram para identificar algumas limitações e dificuldades.

Após a apresentação dos testes, foram detalhados os resultados encontrados, e feita uma análise sobre estes. A primeira dificuldade encontrada foi a escolha da AC Principal, procedimento este, que não foi encontrado na literatura. Foram apresentados os efeitos causados por uma má escolha da AC Principal, assim como foi demonstrado um método para determinar quais ACs irão participar do domínio a partir da escolha de uma determina entidade para realizar a integração.

A montagem do caminho de certificação para validar assinaturas

também foi um tema abordado neste capítulo, onde foram demonstradas as limitações que podem ser causadas, após a integração de duas ICPs, pela falta de uso de um mecanismo automatizado de busca dos certificados pertencentes ao caminho de certificação. Neste trabalho, sugere-se fortemente o uso da extensão *Authority Information Access* para indicar os repositórios com os certificados das ACs.

Alguns dos métodos de integração analisados, não contam com algumas propriedades fundamentais necessárias para integração de dispositivos em massa. Esses métodos foram discutidos, analisados, e foi sugerido a não utilização destes para integração de dispositivos em massa.

Foram feitas análises sobre a necessidade de padronização de algoritmos e formatos de assinaturas. Atualmente existem diversos padrões, só que eles diferem em vários aspectos, ou são muito flexíveis. Estes recursos, muito úteis quando utilizados internamente a uma única ICP, podem acabar inviabilizando a integração entre dispositivos.

Foram propostas também cinco alternativas para viabilizar a validação do carimbo do tempo (geralmente presente em assinaturas de longo prazo) após a saída de algum dos membros do domínio.

Por último, foi feito um comparativo entre a integração de ICPs na visão atual, e na visão defendida neste trabalho; a integração de vários dispositivos.

# 6 ESTUDO DE CASO: ICP-BRASIL

## 6.1 INTRODUÇÃO

A ICP-Brasil foi instituída pela Medida Provisória 2.200-2 [62], de 24 de agosto de 2001. A ICP-Brasil é mantida pelo Instituto Nacional de Tecnologia da Informação (ITI), de acordo com as regras estabelecidas pelo Comitê Gestor da ICP-Brasil (CG). Este comitê é formado por representantes dos poderes da República, de segmentos da sociedade e da academia, os quais são nomeados pelo Presidente da República.

Os certificados digitais emitidos pela ICP-Brasil garantem, por força da legislação, validade jurídica aos atos praticados com seu uso. Isto significa que os certificados da ICP-Brasil podem substituir as assinaturas feitas em documentos de papel, com a mesma eficácia probante, permitindo a desmaterialização dos documentos no Brasil.

A AC-Raiz também está encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviços habilitados na ICP-Brasil. Além disso, verificar se as Autoridades Certificadoras (ACs) estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor [63].

O presente capítulo possui o objetivo de apresentar detalhadamente o cenário atual da ICP-Brasil, e após realizar algumas análises técnicas sobre a infraestrutura. Esta análise objetiva encontrar pontos para futuras melhorias e prever as necessidades a médio e longo prazo. Também serão feitas simulações da integração desta ICP com outras ICPs, utilizando as recomendações feitas no capítulo 5. Esta simulação objetiva verificar se as considerações feitas podem ser aplicadas à integração de domínios governamentais.

## 6.2 CENÁRIO ATUAL

A ICP-Brasil adota uma estrutura hierárquica, composta por uma AC Raiz, e várias ACs subordinadas. A Autoridade Certificadora Raiz é chamada de "Autoridade Certificadora Raiz Brasileira"e é mantida em uma sala-cofre, sem conectividade com o mundo externo. Abaixo da AC Raiz, existem dois níveis de ACs Intermediárias. O primeiro nível formado por ACs que geralmente não possuem conectividade, e estão mais protegidas que as ACs do segundo nível. As ACs do primeiro nível não emitem certificados para os usuários (com exceção da AC da Presidência da República - AC PR[1].). O segundo nível de ACs Intermediárias é o que

[1] A AC PR tem o objetivo de emitir e gerir certificados digitais das autoridades da Presidência da República, ministros de estado, secretários-executivos e assessores jurídicos que se relacio-

| Perfil | Validade (em anos) | Mídia de armazenamento | Processo de geração de chave | Tamanho da chave |
|---|---|---|---|---|
| A1 e S1 | 1 | Software | Software | 1024 |
| A2 e S2 | 2 | Token / Smartcard | Software | 1024 |
| A3 e S3 | 3 | Token / Smartcard / MSC | Hardware | 1024 |
| A4 e S4 | 4 | Token / Smartcard / MSC | Hardware | 2048 |
| T3 | 3 | MSC | Hardware | 1024 |
| T4 | 3 | MSC | Hardware | 2048 |

**Tabela 6.1:** Propriedades dos perfis de certificado da ICP-Brasil

emite certificados diretamente para os usuários, e estas geralmente funcionam conectadas a Internet. O anexo A apresenta as ACs da ICP-Brasil de primeiro e segundo nível, atualizado em 19 de julho de 2010.

Os certificados digitais emitidos pela ICP-Brasil podem ser de 10 perfis: A1, A2, A3, A4, S1, S2, S3, S4, T3, T4 [64]. Os certificados A1, A2, A3 e A4 são para uso exclusivo em aplicações de autenticação e assinatura de documentos. Os certificados S1, S2, S3, S4 são para uso exclusivo em aplicações de cifragem de dados, utilizadas para garantir o sigilo de informações. Os certificados T3 e T4 são para uso exclusivo por autoridades de carimbo de tempo. A tabela 6.1 apresenta resumidamente as propriedades de cada um dos perfis de certificado.

Na tabela 6.1, a primeira coluna representa o tipo do certificado e a segunda coluna demonstra a validade máxima de cada perfil de certificado. A ICP-Brasil possui alguns requisitos mínimos para cada perfil de certificado. Estes requisitos estão resumidos nas três últimas colunas da tabela 6.1. Mais detalhes podem ser encontrados no documento "Requisitos Mínimos para as políticas de certificado na ICP-Brasil"[64].

Atualmente existem quatro ACs raízes na ICP-Brasil, a AC Raiz (Autoridade Certificadora Raiz Brasileira), AC Raiz v1 (Autoridade Certificadora Raiz Brasileira v1), AC Raiz v2 (Autoridade Certificadora Raiz Brasileira v2) e AC Raiz v3 (Autoridade Certificadora Raiz Brasileira v3). Para facilitar a distinção da primeira AC Raiz, a partir deste momento esta será tratada como *AC Raiz v0*.

A tabela 6.2 apresenta os principais campos dos dois primeiros certificados (AC Raiz v0 e AC Raiz v1). A tabela 6.3 apresenta os campos dos dois últimos certificados (AC Raiz v2 e AC Raiz v3).

nem com a PR [63]

| Campo | AC Raiz v0 | AC Raiz v1 |
|---|---|---|
| Versão | 3 | 3 |
| Número Serial | 1 | 4 |
| Nome Comum | Autoridade Certificadora Raiz Brasileira | Autoridade Certificadora Raiz Brasileira v1 |
| Localidade | Brasilia | - |
| Estado | DF | - |
| Organização | ICP-Brasil | ICP-Brasil |
| Unidade Organizacional | Instituto Nacional de Tecnologia da Informacao - ITI | Instituto Nacional de Tecnologia da Informacao - ITI |
| País | BR | BR |
| Validade Inicial | 30/11/2001 | 29/07/2008 |
| Validade Final | 30/11/2011 | 29/07/2021 |
| Algoritmo da Chave | RSA | RSA |
| Tamanho da Chave | 2048 | 2048 |
| Algoritmo de Assinatura | SHA1 + RSA | SHA1 + RSA |

**Tabela 6.2:** Conteúdo dos campos dos certificados das ACs Raízes (v0 e v1) da ICP-Brasil

Através da tabela 6.2 é possível verificar as principais diferenças existentes entre os dois certificados. O número serial do certificado mudou, foi acrescentado "v1"ao nome da segunda AC, e por último, o conteúdo dos campos localidade e estado foram removidos. Comparando-se a validade dos dois certificados é possível verificar que a AC Raiz v1 foi criada quatro meses antes do ponto de atualização (ver seção 3.4.3 da AC Raiz v0.

As extensões dos dois certificados são idênticas. Eles possuem cinco extensões, e as informações delas estão descritas abaixo:

- Extensão *Basic Constraints* - Possui o campo *CA:True*, e não possui o campo *Path Length*;
- Extensão *Subject Key Identifier* - Esta extensão contém o *hash* da chave da respectiva AC Raiz;
- *Key Usage* - Esta extensão possui os usos *Certificate Sign* e *CRL Sign* ativos;
- *CRL Distribution Point* - Esta extensão possui um ponteiro para a URL da LCR da respectiva AC. O repositório utiliza o protocolo HTTP;
- *Certificate Policies* - Esta extensão possui somente um identificador de política, 2.16.76.1.10. Nesta política está associado um qualificador *CPS Pointer*, apontando para a DPC da respectiva AC.

A atualização da AC Raiz, de v0 para v1 não modificou o modo de operação, nem as políticas da AC. A AC Raiz v0 possuía hardware e software criptográfico de empresas estrangeiras. A principal mudança da AC Raiz v1 é que o hardware e software foram desenvolvidos por brasileiros através do projeto João de Barro [65]. No momento de emissão, a AC Raiz v0 também se encontrava próximo ao seu ponto de atualização, criando-se a necessidade de emitir um novo certificado.

O certificados das ACs Raízes v2 e v3 são apresentados na tabela 6.3. A principal diferença entre estes certificados está nos algoritmos utilizados. No primeiro (v2) foi utilizado uma chave de 4096 bits com algoritmo RSA. No segundo, foi utilizado uma chave com algoritmo de curvas elípticas de 521 bits. Ambos os certificados utilizaram a função resumo SHA512.

A diferença entre os certificados das ACs Raízes v2 e v3, em relação ao seu anterior (AC Raiz v1) está nos algoritmos utilizados. Conforme destacado no capítulo 2, os algoritmos utilizados estavam próximos a sua data de expiração, segundo os critérios de validade do NIST, necessitando que uma nova AC fosse emitida com algoritmos mais fortes.

As extensões dos certificados das ACs Raízes v2 e v3 são idênticas, e diferem das extensões das ACs Raízes v0 e v1 apenas pela adição da

| Campo | AC Raiz v2 | AC Raiz v3 |
|---|---|---|
| Versão | 3 | 3 |
| Número Serial | 1 | 1 |
| Nome Comum | Autoridade Certificadora Raiz Brasileira v2 | Autoridade Certificadora Raiz Brasileira v3 |
| Localidade | - | - |
| Estado | - | - |
| Organização | ICP-Brasil | ICP-Brasil |
| Unidade Organizacional | Instituto Nacional de Tecnologia da Informacao - ITI | Instituto Nacional de Tecnologia da Informacao - ITI |
| País | BR | BR |
| Validade Inicial | 21/07/2010 | 21/07/2010 |
| Validade Final | 21/07/2023 | 21/07/2023 |
| Algoritmo da Chave | RSA | ECC (P-521) |
| Tamanho da Chave | 4096 | 521 |
| Algoritmo de Assinatura | SHA512 + RSA | SHA512 + ECDSA |

**Tabela 6.3:** Conteúdo dos campos dos certificados das ACs Raízes (v2 e v3) da ICP-Brasil

extensão *Authority Key Identifier*, que apresenta o identificador da chave da autoridade (o mesmo utilizado na extensão *Subject Key Identifer*).

A AC Raiz v0 possui validade a partir de 30 de novembro de 2001 até 01 de dezembro de 2011, a AC Raiz v1 possui validade desde 29 de julho de 2008 até 29 de julho de 2021 e as ACs Raízes v2 e v3 são válidas desde 21 de junho de 2010 até 21 de junho de 2023. A figura 6.1 demonstra os períodos de validade de uma forma gráfica, através da qual

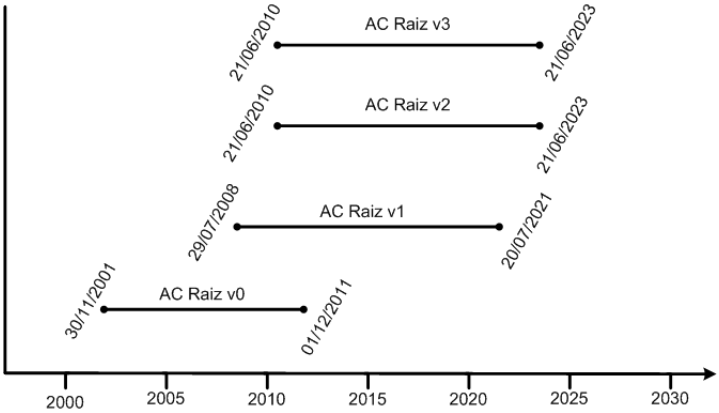


**Figura 6.1:** Período de Validade das ACs Raízes da ICP-Brasil

fica evidente que há períodos em que a ICP-Brasil possui mais de uma AC Raiz válida ao mesmo tempo.

Segundo os documentos "Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil"[64] e "Atribuição de OID na ICP-Brasil"[66], os OIDs de políticas são definidos por tipo de certificado e por entidade. A tabela 6.4, retirada de [64], apresenta como são definidos os OIDs na ICP-Brasil. Cada categoria de certificado possui um OID, em que o último dígito (*n*) identifica a entidade que emitiu o certificado. Por exemplo, um certificado A3 emitido pela "AC Serasa SRF"possui o OID 2.16.76.1.2.3.10, enquanto que um certificado A3 emitido "pela AC CertiSign SRF"possui o OID 2.16.76.1.2.3.6. Esse último dígito, do identificador de política, é atribuído à AC após concluído o seu processo de credenciamento.

## 6.3 ANÁLISE SOBRE O CENÁRIO ATUAL

Esta seção apresenta uma análise sobre o estado atual da ICP-Brasil. Inicialmente serão analisadas e sugeridas melhorias com relação as políticas dos certificados dos usuários. Neste ponto evidencia-se os benefícios que serão alcançados através da implementação da solução proposta neste trabalho.

| Tipo de Certificado | OID |
|---|---|
| A1 | 2.16.76.1.2.1.n |
| A2 | 2.16.76.1.2.2.n |
| A3 | 2.16.76.1.2.3.n |
| A4 | 2.16.76.1.2.4.n |
| T3 | 2.16.76.1.2.303.n |
| T4 | 2.16.76.1.2.304.n |

**Tabela 6.4:** Estrutura dos OIDs de Políticas da ICP-Brasil

### 6.3.1 Análise das Políticas de Certificados da ICP-Brasil

De acordo com o algoritmo de validação do caminho de certificação (que inclui a validação de políticas) citado na RFC5280 [3], a forma como as políticas de certificados estão definidas na ICP-Brasil, torna-os politicamente inválidos, ou seja, não é possível determinar sobre qual políticas os certificados foram emitidos.

Como na AC Raiz está definido apenas um OID de política (2.16.76.1.1.0), todos os certificados emitidos abaixo da AC-Raiz necessitam ser emitidos utilizando esta mesma política para serem validados. O que acontece na ICP-Brasil, é que são definidos outros OIDs de políticas para cada uma das ACs (conforme explicado na seção 6.2). A figura 6.2 apresenta a tela de validação de certificados digitais do Windows 7, mos-

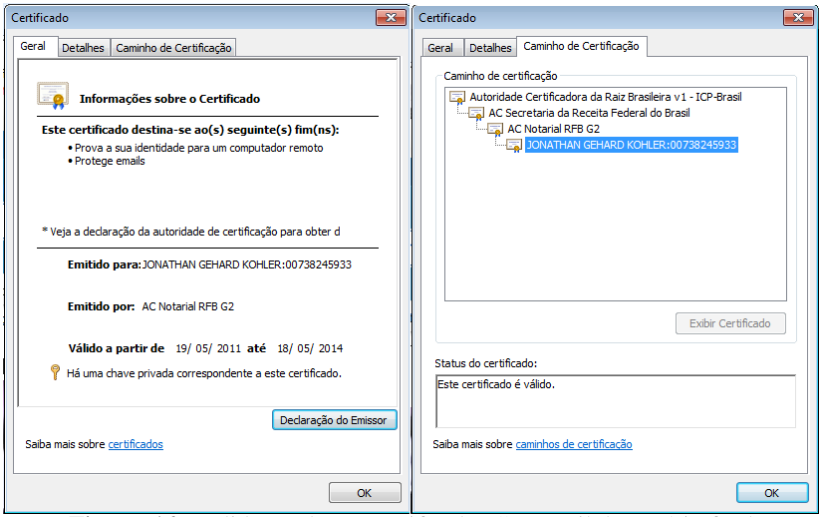


**Figura 6.2:** Validação de um certificado ICP-Brasil de usuário final

trando um certificado A3 de um usuário final. O certificado apresentado

somente é reconhecido como válido para os fins selecionados na extensão *Key Usage*, que são mostrados pelo software como: "Prova a sua identidade para um computador remoto" e "Protege e-mails". Nada é informado sobre qual política o certificado foi emitido, isto é, o Windows não conseguiu reconhecer a política deste certificado.

No exemplo demonstrado na figura 6.2, o OID da política do certificado da AC Raiz é 2.16.76.1.1.0 e o OID da próxima AC (Autoridade Certificadora SERPRO v2) é 2.16.76.1.1.2. A AC Raiz limita o conjunto de políticas válidas em apenas uma política (2.16.76.1.1.). Quando a aplicação verificar a política da segunda AC (2.16.76.1.1.2) esta não vai estar dentro do conjunto de políticas permitidas (que é formado somente pela política 2.16.76.1.1). A intersecção entre os "conjuntos"de políticas da AC Raiz e da AC SERPRO v2 é vazio. Retornando assim, que não existe nenhuma política válida para todo o resto do caminho de certificação.

A política definida no certificado do usuário final somente seria válida se estivesse contida no conjunto que representa a intersecção dos conjuntos de políticas definidas nas ACs do respectivo caminho de certificação (informações mais detalhadas podem ser encontradas na seção 4.5).

Uma forma de implementar estas modificações, seria utilizar o OID especial de políticas *anyPolicy* no certificado da AC Raiz, e os certificados das ACs Intermediárias limitariam o conjunto de políticas disponíveis. As figuras 6.3 e 6.4 apresentam um exemplo desta solução proposta. No certificado da AC Raiz foi definido o OID *AnyPolicy*, conforme pode ser visualizado na figura 6.3, e a aplicação apresenta a política "Todas as diretivas de aplicativo". No certificado da próxima AC foi definido o OID de uma política fictícia (1.2.3.4.5.6.7), e conforme a figura 6.4, a aplicação apresentou esta política como válida. Sendo assim, os certificados emitidos pela AC Intermediária deste exemplo, somente poderiam ser emitidos com a política fictícia 1.2.3.4.5.6.7.

A solução apresentada anteriormente, em que as políticas de certificação não são restringidas no certificado da AC Raiz, permite determinado nível de flexibilidade para futuras modificações nas políticas da infraestrutura. Ao adicionar uma política na infraestrutura, o certificado da AC Raiz não precisa ser modificado, somente os certificados das ACs afetadas pela inclusão desta política. Vale ressaltar que como estas políticas são definidas no certificado das ACs, determinadas mudança nas políticas necessitam da reemissão do certificado desta AC, e a reemissão dos demais certificados afetados.

Também é possível definir o conjunto de todas as políticas da infraestrutura no certificado da AC Raiz, e assim a AC Raiz define as políticas aceitáveis para a infraestrutura através do seu certificado. As figuras 6.5 e 6.6 demonstram a identificação de uma política válida, através de uma AC Raiz com um conjunto de políticas definidas, que depois é restringida pela AC Intermediária.

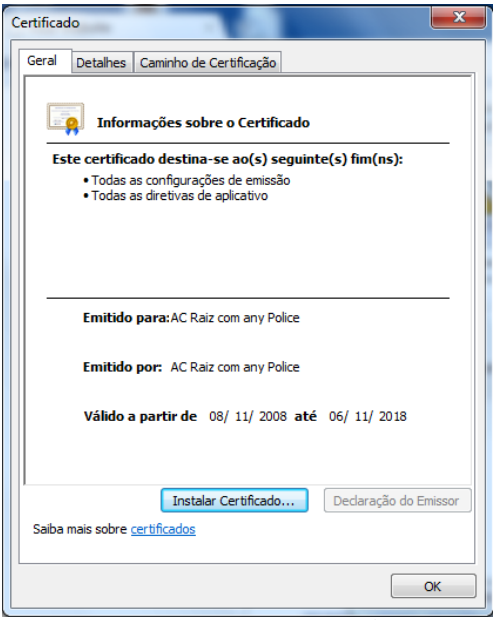


**Figura 6.3:** Certificado digital com política Anypolicy

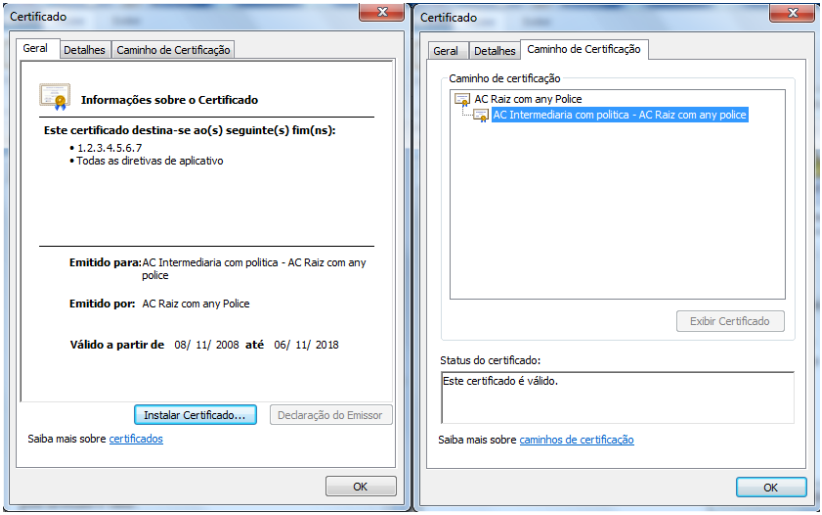


**Figura 6.4:** Certificado digital de AC Intermediária com política válida

Além de modificar a forma como as políticas são definidas no certificado, também sugere-se uma reestruturação da forma como são atribuídos os OIDs de políticas na ICP-Brasil. Atualmente cada OID de

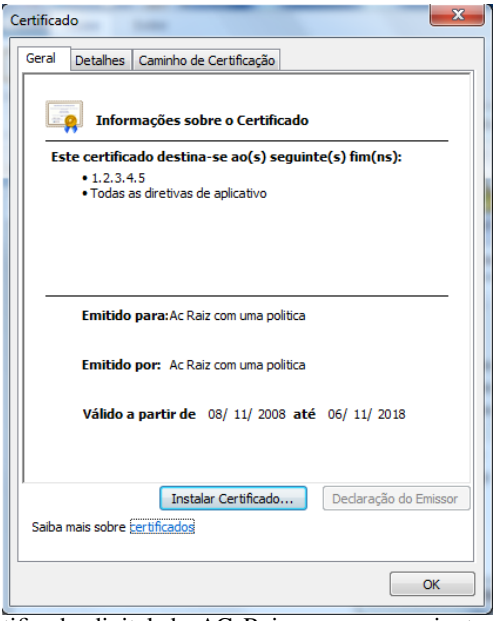


**Figura 6.5:** Certificado digital de AC Raiz com um conjunto de políticas específicas

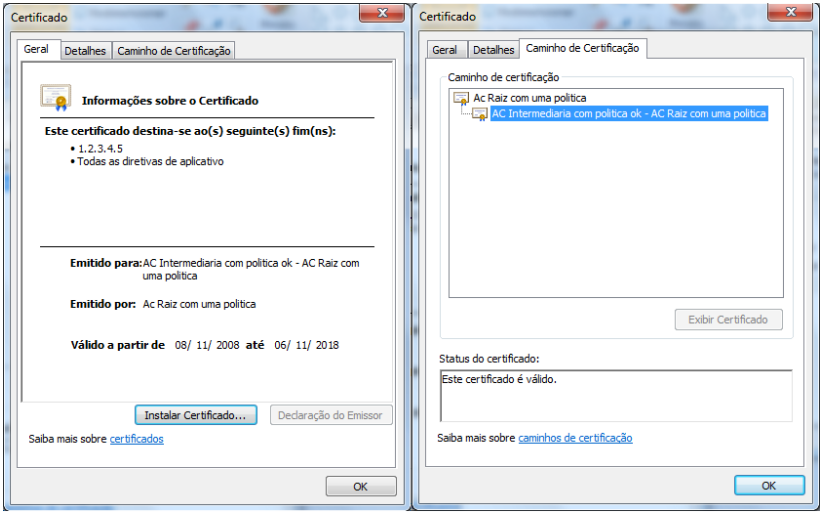


**Figura 6.6:** Certificado digital de AC Intermediária com um conjunto de políticas específicas

política representa uma política específica de uma AC.

Um OID de política, no certificado do usuário, representa um conjunto de requisitos sobre os quais um determinado certificado foi emitido. Como as políticas servem para identificar as classes de certificados de uma infraestrutura, e a ICP-Brasil já possui definido dez perfis de certificados, estes poderiam ser identificados por OIDs de políticas. A cada perfil de certificado é atribuído um OID. E este OID é o mesmo para toda a ICP, diferente da estrutura atual, em que cada política possui um OID diferente para cada AC. Assim, as aplicações conseguiriam identificar qual o perfil de um certificado do usuário, bastando para isso consultar sobre qual política o certificado foi emitido. Por exemplo, uma aplicação que necessite de um alto nível de segurança para efetuar assinatura digitais, somente deveria operar sobre certificados que estão armazenados em um dispositivo criptográfico. Para isto, esta aplicação poderia limitar a utilização de certificados dos perfis A3 ou A4. Como estas políticas já estão definidas, e mudanças não são frequentes, a aplicação necessita conhecer apenas estas dez OIDs, possibilitando identificar todos os perfis de certificados da ICP-Brasil.

A figura 6.7 apresenta um exemplo da estrutura de OIDs de política

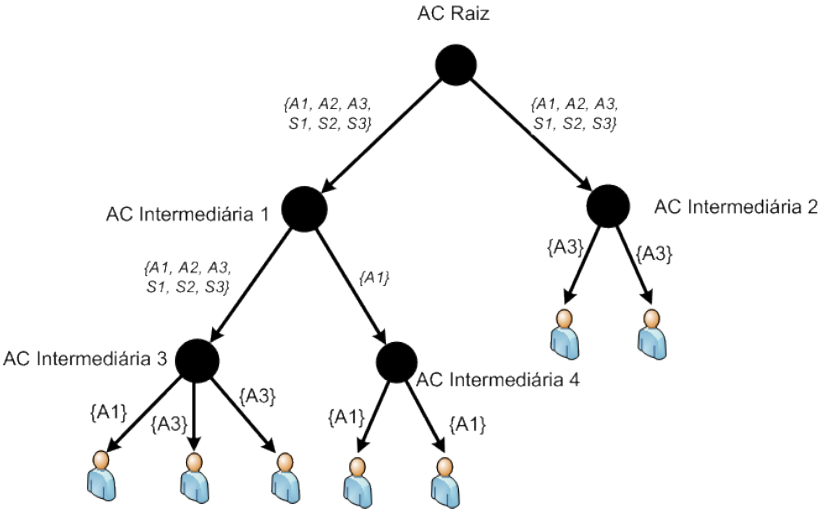


**Figura 6.7:** Estrutura de políticas proposta para ICP-Brasil

proposta neste trabalho. A AC Raiz emite o certificado das ACs Intermediárias de primeiro nível, especificando sobre quais políticas esta AC está autorizada a emitir certificados. Esta, por sua vez, emite o certificado da AC Intermediária de segundo nível delegando alguma (ou todas) políticas, sobre as quais esta AC poderá emitir certificados. No exemplo da figura 6.7, a AC Raiz autorizou as ACs Intermediárias de primeiro nível a emitirem certificados com seis políticas (A1, A2, A3, S1, S2, S3). Na figura, as políticas estão representadas através do nome dos perfis, no

entanto, nos certificados digitais (representados pelas setas) é colocado o OID de cada um dos perfis de políticas. A AC Intermediária 1 delegou a emissão de certificados sobre todas as políticas disponíveis para a AC Intermediária 3, e para a AC Intermediária 4, delegou somente a emissão de certificados sobre a política A1.

Uma alternativa que pode ser implementada, é a utilização do identificador de política *anyPolicy* nos certificados das ACs de primeiro nível. Assim, se no futuro houverem mudanças nas políticas da ICP-Brasil, basta reemitir os certificados das ACs de segundo nível. Vale salientar que se a ICP-Brasil estiver envolvida em algum esquema de integração de ICPs, a mudança nas políticas da ICP-Brasil provavelmente também irá afetar os mapeamentos de políticas desta integração.

### 6.3.2 Análise da validação do caminho de certificação

O algoritmo de validação do caminho de certificação descrito na RFC5280 [3], além de validar os OIDs de políticas, também valida os qualificadores de políticas. Alguns trabalhos, como [8] e [3] desencorajam o uso de qualificadores de políticas. Segundo Housley e Polk [8, p. 90], a utilização de qualificadores de políticas impacta negativamente a interoperabilidade. Por estas razões, recomenda-se fortemente a não utilização de qualificadores de políticas. Se necessário for, sugere-se o uso apenas do qualificador *User Notice*, que não causa grande impacto na interoperabilidade. A utilização do qualificador é fortemente desencorajado, pois a RFC5280 não define como é feito o processamento deste qualificador, apenas definindo que isto é um problema local.

Nes trabalho, sugere-se a exclusão da extensão *CRL Distribution Points* do certificado da AC Raiz. O algoritmo de construção e validação do caminho de certificação descrito na RFC5280 define que o certificado utilizado como ponto de confiança não pertence ao caminho de certificação, portanto este não é validado. O certificado do ponto de confiança somente é utilizado para distribuir a chave pública da entidade, por isso a validade deste certificado não é verificada. Verifica-se apenas a assinatura do certificado. As figuras 6.8 e 6.9 apresentam o certificado de uma AC Raiz revogada sendo validado pelo Windows 7. Mesmo após a importação da LCR, que foi emitida pela AC Raiz revogando o próprio certificado, o certificado continua válido, apresentando o resultado esperado de acordo com o algoritmo definido na RFC5280. O mesmo comportamento foi apresentado no navegador Firefox (rodando no Ubuntu 10.04) e no aplicativo gerenciador de certificados do Mac OS X Snow Leopard.

Atualmente para montar o caminho de certificação dos certificados emitidos pela ICP-Brasil é necessário que os usuários possuam nos seus repositórios de certificados, todos os certificados das ACs da ICP-Brasil. Estes certificados estão disponíveis no sítio da ICP-Brasil. Todavia, com esta solução, a cada vez que uma nova AC for emitida os usuários precisam baixar uma nova versão deste arquivo, e como não há um mecanismo

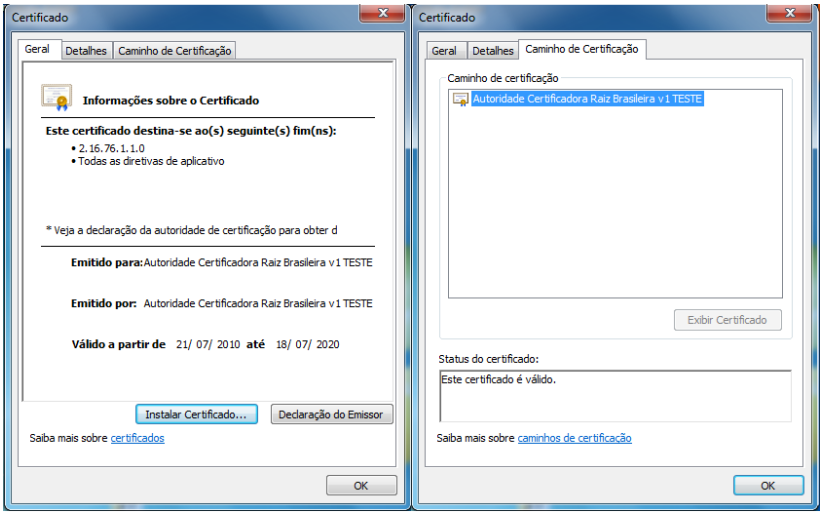


**Figura 6.8:** Certificado de AC Raiz revogado

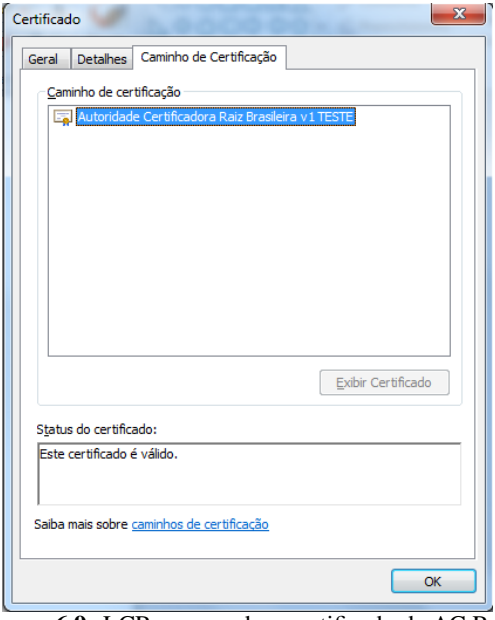


**Figura 6.9:** LCR revogando o certificado de AC Raiz

de notificação de mudanças, os usuários podem não conseguir montar um caminho de certificação pois não possuem a última versão deste arquivo. Esta solução também não é padronizada, sendo assim, não é esperado

que as aplicações baixem regularmente e automaticamente novas versões deste arquivo.

A próxima modificação sugerida por este trabalho, visa combater esta limitação, fazendo a inclusão da extensão *Authority Information Access* (AIA) em todos os certificados da ICP-Brasil, exceto no da AC Raiz. Segundo pesquisa realizada por Pala e Smith[44], menos de 10% dos certificados presentes nos principais navegadores (Firefox, Internet Explorer e Konqueror) e clientes de e-mail (Thunderbird, Outlook e KMail) utilizam a extensão AIA, aumentando a dificuldade das aplicações em acessar os recursos necessários (incluindo os certificados do caminho de certificação)

Esta extensão serve para indicar aonde é possível encontrar o(s) certificado(s) da autoridade emissora do certificado. Por exemplo, no certificado de um usuário, esta extensão aponta para o(s) certificado(s) da AC que emitiu o certificado do usuário. Assim, quando a aplicação for montar o caminho de certificação, ela pode encontrar o certificado da AC através da leitura desta extensão no certificado do usuário. Na próxima iteração do algoritmo de montagem do caminho de certificação, a aplicação vai buscar o certificado da AC que emitiu o certificado da última AC. E assim sucessivamente até chegar ao ponto de confiança do usuário.

A figura 6.10 apresenta o uso da extensão AIA durante a montagem

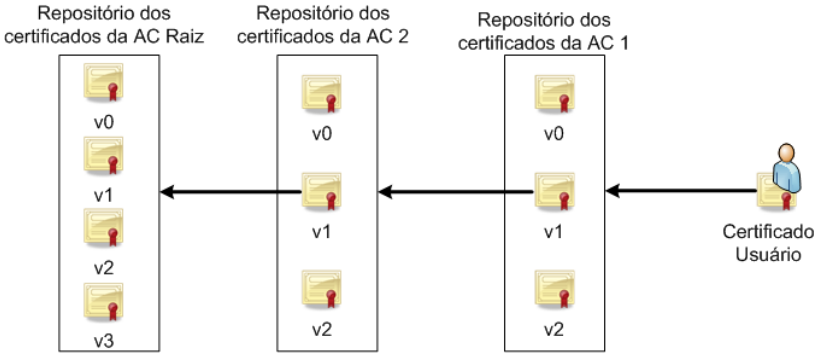


**Figura 6.10:** Uso da extensão AIA na montagem do caminho de certificação

do caminho de certificação. O certificado do usuário possui um ponteiro, através da extensão AIA, para o repositório dos certificados da AC 1, que foi a entidade que emitiu o certificado do usuário. O repositório da AC 1 contém todos os certificados que foram emitidos para esta entidade. A aplicação deve escolher o certificado apropriado desta AC dentre os certificados do repositório. Depois, através da extensão AIA presente no certificado da AC que emitiu o certificado do usuário, a aplicação busca o repositório da próxima AC, e seleciona o certificado adequado. Este procedimento se repete até chegar ao ponto de confiança do usuário. Vale ressaltar que a extensão AIA aponta para um repositório, e não para outro

certificado.

Desta maneira, as aplicações podem, de forma automatizada, baixar da Internet os certificados necessários para montar o caminho de certificação. O usuário também não precisa se preocupar em atualizar o repositório quando novos certificados de ACs são emitidos, pois se o certificado destas novas ACs for necessário, a aplicação pode identificar o local para baixar este certificado.

### 6.3.3 Análise das Políticas de Assinatura da ICP-Brasil

Outro ponto importante a ser considerado é a utilização de Políticas de Assinaturas, as quais são pouco utilizadas por outras ICPs. Se elas forem definidas como obrigatórias para as assinaturas serem consideradas válidas, podem gerar problemas em uma integração com outras ICPs. Isto pode ocorrer devido ao fato que as assinaturas geradas pelas outras ICPs podem não possuir políticas de assinatura, fazendo com que a assinatura seja considerada inválida pelos membros da ICP-Brasil (mas, a assinatura será considerada válida perante os outros membros do domínio que não utilizam políticas de assinatura).

## 6.4 INTEGRAÇÃO ICP-BRASIL E OUTRAS ICPS

A ICP-Brasil atesta a eficácia probante somente dos documentos brasileiros, não contemplando os trâmites de documentos com outros países. Para ocorrer a total desmaterialização dos documentos, se faz necessário criarem-se acordos internacionais para atestar a validade dos documentos brasileiros assinados digitalmente.

Atualmente, já existem iniciativas para viabilizar a troca de documentos digitais com o Brasil. Primeiramente, Portugal despertou o interesse, e depois, em cooperação com a União Européia, surgiu a idéia de realizar a integração dos países participantes do Mercosul, resultando no chamado Mercosul Digital [67].

A integração deste países, pode ser realizada de diversas formas, por eemplo, utilizando as técnicas que foram apresentadas no capítulo 3. No capítulo 5, estas técnicas foram analisadas na visão da integração de muitos dispositivos. Neste mesmo capítulo, também foram feitas algumas recomendações para facilitar, e viabilizar a integração de dispositivos que possuem ICPs internas. Alguns aspectos da integração em massa de dispositivos, são diferentes das atuais análises realizadas sobre a integração de ICPs organizacionais.

As recomendações feitas para a integração de dispositivos foram aplicadas na ICP-Brasil, e contemplando as demais modificações sugeridas neste capítulo, realizaram-se testes para encontrar a melhor forma de integrar a ICP-Brasil com outras ICPs.

### 6.4.1 Simulação da Infraestrutura

Inicialmente foi realizada uma pesquisa sobre a estrutura adotada pelas ICPs dos países pertencentes ao Mercosul. Verificou-se que Chile, Uruguai e Paraguai ainda estão em fase inicial de adoção da tecnologia de certificação digital, e ainda não possuem, ou estão em fases embrionárias de implementação de uma ICP governamental, que seja adotada formalmente em todo o território nacional. Assim, foram feita previsões para estas ICPs, e para aumentar a amplitude deste estudo, foi considerado que estas iriam utilizar diferentes estruturas de certificação e diferentes algoritmos. Para a ICP chilena foi considerado que esta utilizaria a estrutura de malha, a Uruguaia estrutura hierárquica, e para a Paraguai foi escolhida a estrutura de Ponte. Para as ICPs do Uruguai e Paraguai definiu-se algoritmos de curvas elípticas, e a ICP do Chile utilizou-se algoritmos RSA. As ACs principais de cada ICP foram definidas como sendo a AC do ponto de confiança. Por fim, na pesquisa constatou-se que as ICPs Argentina e Venezuelana adotam a estrutura hierárquica com algoritmos RSA.

Após a criação desta estruturas, foram criados os certificados da ICP brasileira. Estes certificados possuem a estrutura sugerida neste trabalho, descrita na seção 6.3.

As ACs Principais escolhidas foram os pontos de confiança de cada ICP. Esta escolha foi feita para assegurar que todos os integrantes das ICPs participassem do domínio integrado.

Após a integração destas infraestruturas, foram geradas assinaturas utilizando os formatos XADES e CADES. Após, foi feita a validação destas assinaturas pelos outros integrantes do domínio. Também foi verificada a autenticação entre os domínios através de um sítio criado especialmente para tal finalidade, que utilizou o protocolo SSL/TLS [68, 69].

Acredita-se que estes domínios serão criados, e continuarão integrados a longo prazo. Para isto, testou-se a criação de novas versões dos pontos de confiança de cada uma das ICPs pertencentes ao domínio.

Durante as simulações foram encontradas algumas dificuldades relativas a montagem do caminho de certificação, já discutidas na seção 5.3.2. Para contorna-las, foram feitas novas simulações, alterando as ICPs a serem integradas de acordo com as sugestões do capítulo 5.

Os resultados obtidos com cada um dos métodos de integração serão detalhados a seguir. As dificuldades que já foram discutidas na seção 5.3 não serão comentadas nas seções a seguir.

#### 6.4.1.1 Autoridades de Confiança

O primeiro método escolhido nos testes para a integração das ICPs dos países do Mercosul, foi a utilização de Autoridades de Confiança. Este mecanismo foi implementado de duas formas: na primeira foi criada uma Autoridade de Confiança que emitiria uma lista periódica com os certificados das ACs Principais pertencentes ao domínio; na segunda foram criadas várias Autoridades de Confiança, cada uma vinculada a

uma ICP. Esta abordagem permite que cada ICP defina o seu conjunto de ICPs confiáveis, podendo optar por não confiar em todos membros. Isto não caracteriza um domínio, pois, quando uma entidade participa de um domínio, ela confia em todos os seus membros.

Na literatura não foi encontrada menção a respeito de um formato padronizado para estas listas de confiança. Durante as simulações, estas listas de confiança foram implementadas utilizando o padrão PKCS#7 [70], que é utilizado amplamente para assinaturas digitais e distribuição de certificados, além de contar com atributos que possibilitam a inclusão de uma lista de certificados digitais.

A primeira limitação encontrada nesta técnica, foi o mapeamento das políticas, que não foi previsto. Sendo assim, para validar uma assinatura digital, era preciso que as aplicações dos usuários de uma ICP conhecessem as políticas da outra ICP.

Outra limitação encontrada foi a falta de suporte desta técnica em várias aplicações, dentre elas: navegadores, editores de texto, clientes de correio eletrônico etc. Devido a esta limitação, não foi possível analisar os impactos gerados nas assinaturas digitais e nos processos de autenticação. Acredita-se que, mesmo com a eliminação desta limitação, esta técnica não é adequada para integrar ICPs, pois não é possível realizar o mapeamento das políticas de um certificado emitido. Esta limitação pode ser contornada emitindo-se certificados entre as ICPs, possibilitando o mapeamento de políticas, porém esta operação caracteriza-se como uma Certificação Cruzada.

#### 6.4.1.2 Autoridade Unificadora

O segundo método testado foi a criação de uma AC Unificadora. Esta foi criada utilizando-se um certificado auto-assinado, com validade de cinco anos, e utilizando os algoritmos sugeridos na seção 2.4.1.

Foram definidas algumas políticas para o domínio integrado, e as políticas das ICPs foram mapeadas nos certificados emitidos para as ACs Principais. Entretanto não foi possível realizar o mapeamento das políticas do domínio para as respectivas políticas de cada ICP. Assim, as políticas identificadas pelas ICPs foram as políticas do domínio.

As assinaturas digitais geradas, foram validadas com sucesso pelos outros integrantes do domínio, mas, foram validadas segundo as políticas do domínio. Esta pode ser uma dificuldade, caso as aplicações somente reconheçam as políticas internas de uma ICP.

As aplicações testadas não tiveram problemas para montar e validar o caminho de certificação utilizando este método de integração. Elas interpretaram o domínio integrado como se fosse uma ICP que utiliza a estrutura hierárquica com uma AC Raiz como ponto de confiança.

A principal desvantagem deste método, conforme descrito em 3.5.1.3, é que esta AC torna-se o ponto de confiança para todos os usuários do domínio. Neste caso, esta AC tornaria-se uma AC multinacional, sendo

responsável pela confiança entre vários países. Na prática, a subordinação de ICPs governamentais a uma AC que não pertence aquele governo, dificilmente é aceita.

#### 6.4.1.3 Certificação Cruzada

Outra técnica testada foi a Certificação Cruzada. No total, foram emitidos 20 certificados, criando relações entre todas as ACs Principais. Durante a emissão destes certificados, é necessário fazer a avaliação e mapeamento das políticas entre as ICPs. Sendo assim, o trabalho de comparação e mapeamento foi realizado 20 vezes, mesmo número de certificados emitidos. Na prática, esta foi a parte mais complicada de ser realizada.

Nas políticas hipotéticas utilizadas, houveram diferentes conceitos, e em determinados casos, foi complicado integrá-los, porém possível. Em uma das políticas, foi suposto que cada política identificaria os certificados de acordo com a sua aplicação: assinatura, autenticação, autoridade certificadora, SSL etc. Em outra política, foi suposto que cada política identificaria o nível de segurança atribuído a chave do certificado: alto, médio ou baixo.

Os certificados cruzadas também possuem validade, e após a sua expiração a integração entre as duas ICPs é desfeita. Como estes certificados são utilizadas apenas para montar um caminho entre duas ICPs, apenas foi necessário emitir um novo certificado antes da expiração do primeiro. Assim, o caminho de certificação passa pelo segundo certificado após o primeiro expirar.

Uma limitação encontrada na utilização deste mecanismo de integração para o Mercosul Digital, é que não é criado um domínio. Cada integrante escolhe em qual ICP vai confiar, e como serão mapeadas as políticas. As aplicações testadas não tiveram problemas para montar e validar o caminho de certificação utilizando este método de integração.

#### 6.4.1.4 Pontes

Outro método de integração simulado foi a Ponte. Inicialmente foi gerada uma AC, com um certificado auto assinado. Este foi utilizado somente para fazer a divulgação da chave pública desta entidade aos outros integrantes do domínio.

A criação da AC Ponte, exigiu que fossem definidas políticas que seriam aplicadas ao domínio. Foi escolhido criarem-se políticas com relação ao nível de segurança empregado na chave do usuário. As políticas do domínio foram definidas em: *baixo*, *médio* e *alto*.

A principal vantagem desta abordagem, foi a diminuição da quantidade de mapeamentos de políticas necessários, diminuindo drasticamente o tempo despendido na análise das políticas das ICPs. Em pontes, a adição de um membro ao domínio, necessita apenas da comparação da política

desta ICP com o domínio, enquanto que na certificação cruzada, era necessário fazer $n$ comparações, onde $n$ é o número de ICPs que já participam do domínio. No teste realizado, foram necessárias 5 comparações.

Uma desvantagem deste método é a criação de um ponto central de falha. Se a AC Ponte for comprometida, o domínio precisa ser desfeito e um novo domínio criado, causando a necessidade da criação de uma nova AC Ponte. Outra desvantagem é o alto custo, pois é necessário a implantação de uma Autoridade Certificadora para fazer a gerência dos membros que fazem parte do domínio.

As aplicações testadas também não tiveram problemas para montar e validar o caminho de certificação utilizando este método de integração.

## 6.5 CONCLUSÃO

Neste capítulo foi apresentado um breve resumo da situação atual da ICP-Brasil, bem como as suas políticas de certificação, também foram apresentado alguns quadros comparativos entre os certificados das ACs raizes da ICP-Brasil.

Após a descrição das principais características da ICP-Brasil, foi feito uma análise, onde foram encontrados algumas dificuldades. Constatou-se que da forma como estão implementadas as políticas de certificação na ICP-Brasil, não é possível definir sobre qual política um certificado foi emitido. A falta desta informação para as aplicações é essencial, pois, é através das políticas que uma aplicação identifica se um certificado está possui os requisitos para ser utilizado. Baseado no algoritmo de validação de caminho de certificação definido da RFC5280, sugerem-se duas modificações sobre a implementação de políticas na ICP-Brasil. Primeiro, a modificação das regras de definição dos identificadores de políticas nos certificados, e segundo, a modificação de como os OIDs de políticas foram atribuídos para as políticas da ICP-Brasil. Sugere-se que cada perfil de certificado (A1, A3, S1, S2 etc.) possua um único OID de política para toda a árvore de certificação. Conforme demonstrado durante este capítulo, com estas modificações propostas, as aplicações podem determinar sob quais políticas um certificado foi emitido.

Outra modificação sugerida neste trabalho, foi a inclusão da extensão AIA nos certificados, para facilitar a montagem do caminho de certificação pelas aplicações.

Por último, foi realizado uma simulação da integração da ICP-Brasil com outras ICPs. Esta simulação objetivou verificar se as modificações sugeridas anteriormente neste capítulo, iriam aumentar a complexidade na integração da ICP-Brasil com outros domínios. Os estudos realizados, apontam que diversas alternativas podem ser utilizadas, cada qual com os seus benefícios e limitações.

Considerando-se que o custo de implantação e manutenção de uma AC Ponte não é demasiadamente oneroso para o Mercosul Digital, do ponto de vista técnico, sugere-se que seja utilizada a técnica de

integração através de Pontes. Porém, impasses entre os membros, como a determinação de um local físico para sediar a AC Ponte, podem levar a escolha da técnica de Certificação Cruzada. Outras técnicas (LCC, Autoridades de Confiança e Autoridade Unificadora) não são recomendadas pois não suportam o mapeamento de políticas.

# 7 CONSIDERAÇÕES FINAIS

Os atuais modelos de certificação digital foram concebidos baseando-se na premissa que haveriam poucas ICPs, e que estas seriam, em sua maioria, grandes infraestruturas compostas por diversas ACs. Esses também consideram que a integração entre ICPs não é uma operação realizada com frequência, sendo executada dependente da interação humana.

Como foi apresentado no capitulo 1, já houve tentativas de integração entre algumas organizações, como a *US Federal PKI* [10], a ICP da união européia [11], e mais recentemente a ICP japonesa [12]. Os resultados encontrados por estes projetos foram muito bons, no entanto, alguns aspectos ainda não foram totalmente resolvidos.

Neste trabalho, além dos aspectos de integração, defende-se que no futuro existirão ICPs internas em diversos dispositivos (que possuem um mínimo poder computacional). Frequentemente estes dispositivos precisarão realizar trocas de mensagens, ou autenticações. Para realizar tais operações, é necessário integrar estas ICPs a *priori*. Estas considerações alteram diversas características fundamentais em que os estudos já realizados estavam focados.

Este trabalho teve como principal objetivo esclarecer os mecanismos de integração de ICPs atuais, e validá-los sobre o ponto de vista da integração de dispositivos. O principal ponto considerado nas análises foi a gestão das políticas de certificação e algoritmos a longo prazo.

Inicialmente foram estudados e analisados os mecanismos mais utilizados de integração descritos na literatura especializada. Também foi verificada a existência de trabalhos relacionados, mas estes não se encontram em estágios que permitam executar análises completas sobre uma integração massiva de ICPs. Foram levantados os principais projetos e resultados de pesquisas realizadas sobre a integração de domínios existentes, porém estes estudos não foram realizados com base na necessidade de integrar muitos dispositivos. Também foram estudados os mecanismos de gerenciamento de âncoras de confiança.

A principal contribuição deste trabalho foi realizar um estudo, além de simulações, para verificar a possibilidade de integração de vários dispositivos. Neste estudo foram avaliados os efeitos causados sobre as assinaturas digitais e os processos de autenticação, bem como o seu comportamento em alguns softwares disponíveis atualmente. Foram consideradas as assinaturas de curto e longo prazo, incluindo assinaturas que deveriam continuar válidas mesmo após a dissolução do domínio.

Concluiu-se que as pesquisas realizadas anteriormente não eram suficientes, e os novos estudos realizados demonstraram que a integração de ICPs ainda possui algumas lacunas, que precisam ser sanadas para possibilitar a integração de dispositivos em massa. Estes resultados, e

suas respectivas análises, estão descritos em detalhes no capítulo 5.

Ao realizar estudos sobre quais aspectos precisam ser avaliados ao integrar ICPs, foram considerados as diferenças entre algoritmos existentes entre dois domínios. O capítulo 2 apresentou uma visão geral sobre os atuais algoritmos, e discutiu sobre as padronizações e recomendações mais utilizadas atualmente. Estas recomendações divergem em alguns algoritmos recomendados, entretanto. conforme verificado nas simulações realizadas no capítulo 5, estas não apresentaram restrições na integração de domínios, desde que o algoritmo seja suportado pelas aplicações.

Durante o decorrer deste trabalho foram encontradas algumas dificuldades. A primeira foi como efetuar a escolha da melhor AC para realizar os processos de integração, e quais os seus efeitos. Foi apresentado um método para determinar a abrangência de entidades que pertencerão ao domínio integrado, de acordo com a escolha da AC. Também foram feitas algumas considerações sobre a escolha, considerando as diferenças entre os modelos de hierarquias de ICPs.

Outra dificuldade foi a montagem do caminho de certificação após os domínios serem integrados. Conforme explanado no capítulo 5, para contornar este problema é necessário algum método que seja padronizado e automatizado para buscar os certificados necessários para a montagem do caminho de certificado. Ainda neste tópico, foi abordado a integração de domínios de domínios, a qual dificulta ainda mais a validação de assinaturas digitais sem a utilização de um método para tal. Neste trabalho é recomendado a utilização da extensão *Authority Information Access* (AIA), conforme detalhado nos capítulos 3 e 5.

Outro ponto importante do trabalho foi o estudo realizado sobre o gerenciamento e mapeamento das políticas nestes domínios. A principal dificuldade encontrada foi realizar o mapeamento das políticas. Algumas ICPs apresentaram diferentes conceitos para caracterizar os níveis de políticas, dificultando encontrar uma relação de equivalência. Foram pesquisados mecanismos que automatizam este processo, no entanto os trabalhos encontrados estavam em fase embrionária, não abrangendo as necessidades deste trabalho. As políticas de certificação foram explicadas (capítulo 4). Foram analisadas, e considerações acerca de como implementá-las, além de cuidados necessários, foram feitas no capítulo 5. A principal dificuldade encontrada no tratamento de políticas foi o mapeamento automático, principal fator limitante para a integração em massa de dispositivos.

Alguns dos métodos analisados, como LCC e Autoridades de Confiança, devido ao modo como foram propostos, não permitem que seja realizado o mapeamento de políticas.

Além dos algoritmos criptográficos empregados para realizar assinaturas digitais, são necessários padrões que definem a estrutura de uma assinatura digital. Estes formatos foram analisados, e foram apresentados os impactos causados pela diversidade de padrões na integração de ICPs.

Um dos pontos em que foi encontrada maior dificuldade foi a

preservação de documentos a longo prazo, especialmente aqueles que precisam continuar válidos mesmo após a saída de algum membro do domínio. Este trabalho apresentou um passo inicial para a solução deste problema através da criação de cinco alternativas. Assim, a manutenção da validade de documentos após a dissolução dos integrantes de um domínio pode ser garantida, já que agora esta pode ser realizada de várias formas.

Por último, foi realizado um estudo de caso sobre a integração da ICP-Brasil com outras infraestruturas. Este estudo foi motivado por iniciativas já existentes entre Brasil e outros Países. Neste estudo foram sugeridas melhorias a serem realizadas na ICP-Brasil que facilitariam a integração desta com outras ICPs. A maior parte das sugestões tomaram como base o estudo realizado anteriormente sobre a integração de dispositivos móveis.

Como trabalhos futuros, podem ser exploradas algumas das limitações deste trabalho, descritas no capítulo 1. Os próximos passos para facilitar a integração em massa de dispositivos, na visão do autor, é a criação de um método de mapeamento automático de políticas totalmente automatizável, além da definição de um padrão-comum para a interoperabilidade entre ICPs. Eliminando os problemas de interoperabilidade causados pela implementação de aplicativos que seguem diferentes padrões criados com o mesmo objetivo. Outra oportunidade aberta por este trabalho é a realização de um estudo de caso, ou projeto piloto, com fabricantes de dispositivos para detectar dificuldades na comunicação intra-dispositivos. Este pode auxiliar também na criação de uma interface padronizada para comunicação entre dispositivos de diferentes fabricantes, e com diferentes funcionalidades.

## REFERÊNCIAS


[1] BARKER, E. et al. *Recommendation for Key Management - Pat1: General (Revised)*. [S.l.], Mar 2007. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf>.

[2] BARKER, E. et al. *Recommendation for key Management - Part 3: Application-Specific Key Management Guidance*. [S.l.], Dez 2009. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf>.

[3] COOPER, D. et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF, maio 2008. RFC 5280 (Proposed Standard). (Request for Comments, 5280). Disponível em: <http://www.ietf.org/rfc/rfc5280.txt>.

[4] MYERS, M. et al. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. IETF, jun. 1999. RFC 2560 (Proposed Standard). (Request for Comments, 2560). Disponível em: <http://www.ietf.org/rfc/rfc2560.txt>.

[5] FREEMAN, T. et al. *Server-Based Certificate Validation Protocol (SCVP)*. IETF, dez. 2007. RFC 5055 (Proposed Standard). (Request for Comments, 5055). Disponível em: <http://www.ietf.org/rfc/rfc5055.txt>.

[6] KONFELDER, L. *A method for certification*. Cambridge, Massachusetts, Maio 1978.

[7] ITU-T. *X.509 : Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks*. nov. 2008. (Recommendation).

[8] HOUSLEY, R.; POLK, T. *Planning for PKI - Best Practices Guide for Deploying Public Key Infrastructure*. New York: Wiley Computer Publishing, 2001.

[9] ICPEDU. *Infraestrutura de Chaves Públicas para Ensino e Pesquisa - ICPEDU*. 2010. Disponível em: <http://www.icp.edu.br>. Acesso em: 18 Dez. 2010.

[10] ALTERMAN, P. The us federal pki and the federal bridge certification authority. *Comput. Netw.*, Elsevier North-Holland, Inc., New York, NY, USA, v. 37, p. 685–690, December 2001. ISSN 1389-1286. Disponível em: <http://portal.acm.org/citation.cfm?id=567404.567405>.

[11] EBCA. *European Bridge-CA*. Disponível em: <http://www.bridge-ca.org>. Acesso em: 15 Dez. 2010.

[12] MIYAKAWA, Y. et al. Current status of japanese government pki systems. In: *Proceedings of the 5th European PKI workshop on Public Key Infrastructure: Theory and Practice*. Berlin, Heidelberg: Springer-Verlag, 2008. (EuroPKI '08), p. 104–117. ISBN 978-3-540-69484-7. Disponível em: <http://dx.doi.org/10.1007/978-3-540-69485-4_8>.

[13] CALLAS, J. et al. *OpenPGP Message Format*. IETF, nov. 2007. RFC 4880 (Proposed Standard). (Request for Comments, 4880). Updated by RFC 5581. Disponível em: <http://www.ietf.org/rfc/rfc4880.txt>.

[14] ELLISON, C. *SPKI Requirements*. IETF, set. 1999. RFC 2692 (Experimental). (Request for Comments, 2692). Disponível em: <http://www.ietf.org/rfc/rfc2692.txt>.

[15] ELLISON, C. et al. *SPKI Certificate Theory*. IETF, set. 1999. RFC 2693 (Experimental). (Request for Comments, 2693). Disponível em: <http://www.ietf.org/rfc/rfc2693.txt>.

[16] OPENSSL. *OpenSSL: The Open Source toolkit for SSL/TLS*. 2010. Disponível em: <http://www.openssl.org>. Acesso em: 18 Dez. 2010.

[17] BOUNCY CASTLE. *Bouncy Castle Crypto APIs*. 2010. Disponível em: <http://www.bouncycastle.org/>. Acesso em: 18 Dez. 2010.

[18] ORACLE CORPORATION. *Java Cryptography Architecture*. 2010. Disponível em: <http://download.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpec.html>. Acesso em: 18 Dez. 2010.

[19] MOZILLA FOUNDATION. *Network Security Services (NSS)*. 2010. Disponível em: <http://www.mozilla.org/projects/security/pki/nss/>. Acesso em: 18 Dez. 2010.

[20] MICROSOFT CORPORATION. *Cryptography API: Next Generation*. Set. 2010. Disponível em: <http://msdn.microsoft.com/en-us/library/aa376210.aspx>. Acesso em: 18 Dez. 2010.

[21] DIFFIE, W.; HELLMAN, M. E. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22, n. 6, p. 644–654, 1976. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.37.9720>.

[22] GUTMANN, P. Pki: it's not dead, just resting. *Computer*, v. 35, n. 8, p. 41 – 49, ago. 2002. ISSN 0018-9162.

[23] GUTMANN, P. Plug-and-play pki: a pki your mother can use. In: *Proceedings of the 12th conference on USENIX Security Symposium - Volume 12*. Berkeley, CA, USA: USENIX Association, 2003. p. 4–4. Disponível em: <http://portal.acm.org/citation.cfm?id=1251353.1251357>.

[24] WILSON, S. Public key superstructure "it's pki jim, but not as we know it!". In: *Proceedings of the 7th symposium on Identity and trust on the Internet*. New York, NY, USA: ACM, 2008. (IDtrust '08), p. 72–88. ISBN 978-1-60558-066-1. Disponível em: <http://doi.acm.org/10.1145/1373290.1373301>.

[25] HANNA, S. R.; PAWLUK, J. Identifying and overcoming obstacles to pki deployment and usage. In: *Proceedings of the 3rd Annual PKI R&D Workshop*. [S.l.: s.n.], 2004.

[26] RIVEST, R. L.; LAMPSON, B. *A Simple Distributed Security Infrastructure (SDSI)*. 1996. Disponível em: <http://groups.csail.mit.edu/cis/sdsi.html>. Acesso em: 18 Dez. 2010.

[27] FERREIRA, J. da Silva Fraga e Frank Siqueira e Carla M. Westphall e Altair Santin e Michelle Wangham e Emerson Mello e Laura Carrijo e D. R. *Trust Chains Project*. 2000. Disponível em: <http://gcseg.das.ufsc.br/cadconf/index-en.html>. Acesso em: 28 Dez. 2010.

[28] LI, B.; DAI, K.; ZHANG, S. Virtual certificate authority for virtual enterprises. *Advanced Issues of E-Commerce and Web-Based Information Systems, International Workshop on*, IEEE Computer Society, Los Alamitos, CA, USA, v. 0, p. 0222, 2001.

[29] GUO, Z.; OKUYAMA, T.; FINLEY, M. R. J. A new trust model for pki interoperability. In: *Proceedings of the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services*. Washington, DC, USA: IEEE Computer Society, 2005. p. 37–. ISBN 0-7695-2450-8. Disponível em: <http://portal.acm.org/citation.cfm?id=1105923.1105969>.

[30] BICKENBACH, H.-J. et al. *Common PKI Specifications for Interoperable Applications - v.2.0*. [S.l.], Jan. 2009. Disponível em: <http://www.t7ev.org/uploads/media/Common-PKI_v2.0_02.pdf>.

[31] SHIMAOKA, M.; HASTINGS, N.; NIELSEN, R. *Memorandum for Multi-Domain Public Key Infrastructure Interoperability*. IETF, jul. 2008. RFC 5217 (Informational). (Request for Comments, 5217). Disponível em: <http://www.ietf.org/rfc/rfc5217.txt>.

[32] BARKER, W. C. *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (Revised)*. [S.l.], May 2008. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf>.

[33] NIST. *Federal Information Processing Standards (FIPS) Publication 197*. [S.l.], Nov 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[34] GALLAGHER, P.; FOREWORD, D. D.; DIRECTOR, C. F. *FIPS PUB 186-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Digital Signature Standard (DSS)*. [S.l.], June 2009. Disponível em: <http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf>.

[35] HANKERSON, D.; MENEZES, A.; VANSTONE, S. *Guide to elliptic curve cryptography*. [S.l.]: Springer, 2004. ISBN 0-387-95273-X.

[36] CRYPTO-WORLD. *Integer Factoring Records*. 2009. Disponível em: <http://www.crypto-world.com/FactorRecords.html>. Acesso em: 14 jul. 2010.

[37] BARKER, E. et al. *Recommendation for Key Management - Pat1: General (Revised)*. [S.l.], Mar 2007. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf>.

[38] SHIREY, R. *Internet Security Glossary, Version 2*. IETF, ago. 2007. RFC 4949 (Informational). (Request for Comments, 4949). Disponível em: <http://www.ietf.org/rfc/rfc4949.txt>.

[39] CARLOS, M. C. *Topologias dinâmicas de Infra-estrutura de Chaves Públicas*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2007.

[40] MYERS, M. et al. *Certificate Management Messages over CMS*. IETF, abr. 2000. RFC 2797 (Proposed Standard). (Request for Comments, 2797). Obsoleted by RFC 5272. Disponível em: <http://www.ietf.org/rfc/rfc2797.txt>.

[41] FREED, N. *Sieve Email Filtering: Date and Index Extensions*. IETF, jul. 2008. RFC 5260 (Proposed Standard). (Request for Comments, 5260). Disponível em: <http://www.ietf.org/rfc/rfc5260.txt>.

[42] VIGIL, M. A. G. *Infraestrutura de Chaves Públicas Otimizadora*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, 2010.

[43] ADAMS, C. et al. *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. IETF, ago. 2001. RFC 3161 (Proposed Standard). (Request for Comments, 3161). Updated by RFC 5816. Disponível em: <http://www.ietf.org/rfc/rfc3161.txt>.

[44] PALA, M.; SMITH, S. W. Finding the pki needles in the internet haystack. *Journal of Computer Security*, IOS Press, v. 18, n. 3, p. 397–420, Maio 2010.

[45] CHOKHANI, S. et al. *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. IETF, nov. 2003. RFC 3647 (Informational). (Request for Comments, 3647). Disponível em: <http://www.ietf.org/rfc/rfc3647.txt>.

[46] SCHMEH, K. A critical view on rfc 3647. In: *Proceedings of the 4th European PKI workshop on Public Key Infrastructure: Theory and Practice*. Berlin, Heidelberg: Springer-Verlag, 2007. (EuroPKI '07), p. 369–374.

[47] CHOKHANI, S.; FORD, W. *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. IETF, mar. 1999. RFC 2527 (Informational). (Request for Comments, 2527). Obsoleted by RFC 3647. Disponível em: <http://www.ietf.org/rfc/rfc2527.txt>.

[48] W3C. *XML Signature Syntax and Processing (Second Edition)*. [S.l.], jun. 2008.

[49] ETSI. *XML Advanced Electronic Signatures (XAdES) - ETSI TS 101 903*. [S.l.], 2009.

[50] PINKAS, D.; POPE, N.; ROSS, J. *CMS Advanced Electronic Signatures (CAdES)*. IETF, mar. 2008. RFC 5126 (Informational). (Request for Comments, 5126). Disponível em: <http://www.ietf.org/rfc/rfc5126.txt>.

[51] WEAVER, G. A.; REA, S.; SMITH, S. W. Computational techniques for increasing pki policy comprehension by human analysts. In: *Proceedings of the 9th Symposium on Identity and Trust on the Internet*. New York, NY, USA: ACM, 2010. (IDTRUST '10), p. 51–62. ISBN 978-1-60558-895-7. Disponível em: <http://doi.acm.org/10.1145/1750389.1750396>.

[52] CASOLA, V. et al. A policy-based methodology for security evaluation: A security metric for public key infrastructures. *J. Comput. Secur.*, IOS Press, Amsterdam, The Netherlands, The Netherlands, v. 15, p. 197–229, April 2007. ISSN 0926-227X. Disponível em: <http://portal.acm.org/citation.cfm?id=1370659.1370660>.

[53] LI, J. et al. A secure collaboration service for dynamic virtual organizations. *Inf. Sci.*, Elsevier Science Inc., New York, NY, USA, v. 180, p. 3086–3107, September 2010. ISSN 0020-0255. Disponível em: <http://dx.doi.org/10.1016/j.ins.2010.05.014>.

[54] W3C. *Extensible Markup Language (XML)*. 2010. Disponível em: <http://www.w3.org/XML>. Acesso em: 28 Dez. 2010.

[55] COMISSION OF THE EUROPEAN COMMUNITIES. *Action plan on eSignatures and eIdentification to facilitate the provision of cross-border public services in the Single Market*. [S.l.], 2008.

[56] ETSI. *PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES - ETSI TS 102 778-1*. [S.l.], 2009.

[57] ETSI. *PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1 - ETSI TS 102 778-2*. [S.l.], 2009.

[58] ETSI. *PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles - ETSI TS 102 778-3*. [S.l.], 2009.

[59] ETSI. *PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile - ETSI TS 102 778-4*. [S.l.], 2009.

[60] ETSI. *PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures - ETSI TS 102 778-5*. [S.l.], 2009.

[61] EUROPEAN COMISSION - EC. *M/460 EN - Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies applied to Electronic Signatures*. [S.l.], 2009.

[62] MEDIDA PROVISÓRIA N. 2.200-2. Ago 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acesso em: 19 Jul 2010.

[63] ITI, I. N. de Tecnologia da I. *Estrutura da ICP-Brasil*. 2010. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp>. Acesso em: 19 Jul 2010.

[64] ICP-BRASIL. *Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil (DOC-ICP-04), versão 3.1*. [S.l.], abr 2010. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-04_-_Versao_3.1.pdf>. Acesso em: 20 Ago 2010.

[65] ITI, I. N. de Tecnologia da I. *Joao de Barro*. 2010. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Swlivre/JoaoDeBarro>. Acesso em: 29 Dez 2010.

[66] ICP-BRASIL. *Atribuição de OID na ICP-Brasil (DOC-ICP-04.01), versão 2.2*. [S.l.], maio 2010. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-04.01_-_versao_2.2.pdf>. Acesso em: 20 Ago 2010.

[67] MERCOSUL. *Mercosul Digital*. 2010. Disponível em: <http://www.mercosuldigital.org/>. Acesso em: 28 Dez. 2010.

[68] BROWN, M.; HOUSLEY, R. *Transport Layer Security (TLS) Authorization Extensions*. IETF, maio 2010. RFC 5878 (Experimental). (Request for Comments, 5878). Disponível em: <http://www.ietf.org/rfc/rfc5878.txt>.

[69] RESCORLA, E. et al. *Transport Layer Security (TLS) Renegotiation Indication Extension*. IETF, fev. 2010. RFC 5746 (Proposed Standard). (Request for Comments, 5746). Disponível em: <http://www.ietf.org/rfc/rfc5746.txt>.

[70] KALISKI, B. *PKCS #7: Cryptographic Message Syntax Version 1.5*. IETF, mar. 1998. RFC 2315 (Informational). (Request for Comments, 2315). Disponível em: <http://www.ietf.org/rfc/rfc2315.txt>.

# ANEXOS

# A ESTRUTURA DA ICPBRASIL