Universidade Estadual de Campinas
Instituto de Computação

Wylber Polonini

Validação Eficiente de Certificados Digitais

CAMPINAS
2007

Wylber Polonini

Validação Eficiente de Certificados Digitais

Dissertação apresentada ao Instituto de Computação da Universidade Estadual de Campinas como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

Orientador: Prof. Dr. Ricardo Dahab

Este exemplar corresponde à versão final da Dissertação defendida por Wylber Polonini e orientada pelo Prof. Dr. Ricardo Dahab.

CAMPINAS
2007

Agência(s) de fomento e nº(s) de processo(s): CNPq, 131810/2005-7; CAPES

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

P767v

Polonini, Wylber, 1981-
Validação eficiente de certificados digitais / Wylber Polonini. – Campinas, SP : [s.n.], 2007.

Orientador: Ricardo Dahab.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Computação.

1. Criptografia. 2. Infraestrutura de chaves públicas (Segurança do computador). I. Dahab, Ricardo,1957-. II. Universidade Estadual de Campinas. Instituto de Computação. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Efficient digital certificate validation
Palavras-chave em inglês:
Cryptography
Public key infrastructure (Computer security)
Área de concentração: Ciência da Computação
Titulação: Mestre em Ciência da Computação
Banca examinadora:
Ricardo Dahab [Orientador]
Ricardo Felipe Custódio
Julio César López Hernández
Data de defesa: 23-03-2007
Programa de Pós-Graduação: Ciência da Computação

Universidade Estadual de Campinas
Instituto de Computação

Wylber Polonini

Validação Eficiente de Certificados Digitais

Banca Examinadora:

- Prof. Dr. Ricardo Dahab (Orientador)
  Universidade Estadual de Campinas
- Prof. Dr. Ricardo Felipe Custódio
  Universidade Federal de Santa Catarina
- Prof. Dr. Julio César López Hernández
  Universidade Estadual de Campinas

A ata da defesa com as respectivas assinaturas dos membros da banca encontra-se no processo de vida acadêmica do aluno.

Campinas, 23 de março de 2007

Agradecimentos

Eu gostaria de agradecer a todos que contribuíram para o desenvolvimento desse trabalho, em especial:

- aos meus pais, José e Inêz, que sempre me incentivaram e, em muitas vezes, sacrificaram seus objetivos para que os meus fossem alcançados. Logo, essa também é uma conquista deles. Agradeço a minha irmã, Jossana, porque ... ah ... bem ... porque ela é minha irmã. Apenas uma brincadeira com quem sempre se mostra alegre e transmite essa alegria a todos, inclusive a mim;

- ao meu caro orientador Ricardo Dahab por sempre se mostrar atencioso e compreensivo. Também não posso deixar de agradecê-lo por sua enorme contribuição para o desenvolvimento desse trabalho, sempre me guiando;

- aos professores Ricardo Felipe Custódio e Julio C. López-Hernández pelas sugestões dadas, que contribuíram para melhorar esse trabalho;

- à CAPES e ao CNPq por terem financiado esse trabalho;

- a todos os funcionários e professores do Instituto de Computação;

- aos colegas e amigos do IC, em especial aos da turma MSC2004. Como são muitos, não citarei nomes para não correr o risco de esquecer alguém;

- aos amigos da república Quase Mil: Bine, Gabriela, Javier, Leso, Márcia, Matheus, Maurício, Soraya e Tiago;

- aos colegas da Dired, pelo incentivo e "pressão".

Resumo

A validação de certificados digitais é um processo naturalmente custoso, pois envolve operações de criptografia assimétrica, que por sua vez envolvem operações aritméticas cujo tamanho dos operandos é da ordem de milhares de bits. Em alguns casos, dependendo da topologia da infraestrutura de chaves pública (ICP) e dos usuários envolvidos, validar um certificado implica validar uma cadeia de certificados, denominada caminho de certificação, aumentando ainda mais o custo de validação do certificado em questão. No sentido de tornar o processo de validação de certificados digitais mais eficiente, vários mecanismos foram propostos nos últimos anos. Os mais importantes são: NOVOMODO [26], CRT [17], 23CRT [28], ICPA [20], EFFECT [14] e certificados efêmeros [31]. Neste trabalho, as vantagens e desvantagens desses mecanismos são discutidas assim como seus custos, especialmente sobre a ótica de validar um caminho de certificação. Dá-se destaque à ICPA, que permite otimizar a validação dos caminhos de certificação através da supressão parcial da necessidade de se verificar informações de revogação e da substituição de operações assimétricas por operações de *hash*. Também é levantada a questão do custo de emissão de certificados aninhados na ICPA, o que pode torná-la inadequada para ambientes em que o número de usuários é muito grande. Finalmente, introduz-se uma modificação à ICPA, ICPAm, cujo objetivo principal é reduzir o custo de emissão de certificados aninhados, sem aumentar significativamente o custo de validação do caminho de certificação. Na ICPAm, diferentemente do que ocorre na IPCA, as ACs superiores não emitem certificados aninhados quando suas filhas emitem certificados para usuários finais. Consequentemente, o custo de emissão dos certificados aninhados é reduzido.

Abstract

The digital certificate validation process is very costly because it involves asymmetric cryptographic operations which involve arithmetic operations whose operands have more than a hundred bits. In some cases, depending on the public-key infrastructure (PKI) topology and its number of users, validating a certificate means validation of a chain of certificates, known as a certification path, further increasing the cost of validating the target certificate. To make this process less costly, a lot of mechanisms have been proposed in recent years. The most important are: NOVOMODO [26], CRT [17], 23CRT [28], ICPA [20], EFFECT [14] and short lived certificates [31]. In this thesis, the advantages and disadvantages of these mechanisms are discussed as well as their costs, emphasizing the cost of validating a certification path. We give special attention to NPKI, which permits the optimization of certification path validation, partially suppressing the necessity of verifying certificate revocation information and replacing asymmetric cryptographic operations with cryptographic hash operations. We also discuss the nested certificate emission costs in a NPKI, which can make NPKIs not practical for environments where there are a great number of users. Finally, we introduce a modification to NPKIs, the ICPAm, whose objective is to reduce nested certificate emission costs without increasing significantly the certification path validation costs. On the ICPAm, differently from ICPA, the superiors CAs do not emit nested certificate when its daughters CAs emit certificates to end users. Consequently, the nested certificate emission costs are reduced.

Lista de Figuras

Lista de Tabelas

Lista de Abreviações e Siglas

AC	Autoridade Certificadora.
ASR	Acrônimo para os elementos que compõem uma ICP (AC, servidor de informação de revogação, repositório de certificados, etc.), exceto o verificador.
CA	Do inglês *Certification Authority*. É o mesmo que AC.
ICP	Infraestrutura de chaves públicas.
IR	Informação de Revogação.
PGP	Do inglês *Pretty Good Privacy*.
SDSI	Do inglês *Simple Distributed Security Infrastructure*.
SIR	Servidor de Informação de Revogação.
SPKI	Do inglês *Simple Public-Key Infrastructure*.
TPC	Terceira Parte Confiável.
TTP	Do inglês *Trusted Third Party*. É o mesmo que TPC.

Lista de Símbolos

Δ	Conjunto contendo todas as ACs de uma ICP/ICPA/ICPAm.
Θ	Conjunto contendo todos os usuários de uma ICP/ICPA/ICPAm.
C_A	É o custo de operações criptográficas do ASR para criar os certificados e as informações de revogação.
C_C	É o custo das operações criptográficas necessárias à verificação dos certificados.
C_D	É o custo do ASR para gerar e disponibilizar aos verificadores os dados necessários à validação dos certificados.
C_E	É o custo do verificador para extrair e processar as informações contidas nos certificados e nas informações de revogação.
C_M	É o custo do ASR de montar os certificados e as informações de revogação, ou seja, o custo para criar as estruturas de dados que serão assinadas posteriormente, dando origem aos certificados e informações de revogação.
C_R	É o custo de transmissão do verificador para obter os certificados e as informações de revogação.
C_T	É o custo do ASR para transmitir as informações de revogação e os certificados.
C_V	É o custo computacional do verificador para validação de certificados.
k	Número de certificados que compõem o caminho de certificação.
j	Taxa de atualização das informações de revogação. Indica a frequência com que as informações de revogação são divulgadas, medida em ocorrências em um determinado intervalo, por exemplo, hora, dia, semana, etc.
P	Fator de custo adicional de emissão de certificados aninhados.
q	Número de requisições feitas ao servidor de informação de revogação num determinado intervalo de tempo.

r	Número médio de certificados revogados por AC, cujo prazo de validade ainda não tenha expirado.
$\|res\|$	Tamanho do resumo.
$\|sn\|$	Tamanho do número de série do certificado.
$\|sig\|$	Tamanho da assinatura digital.
T_{res}	Tempo para computar uma função de resumo criptográfico.
t	Tempo médio de vida do certificado.
T_{sig}	Tempo para computar uma assinatura digital.
T_{ver}	Tempo para verificar uma assinatura digital.
T_{res}	Tempo para efetuar uma operação de resumo.
v	Número médio de certificados tradicionais gerenciados pela AC.
v_{cn}	Número médio de certificados aninhados gerenciados pela AC.

Sumário

Capítulo 1

Introdução

Motivação

A Criptografia é a principal fonte de mecanismos para prover a troca segura de informações num ambiente inseguro, como a Internet, isto é, com privacidade, integridade e autenticidade (ver Capítulo 2). No que toca a criptografia assimétrica, ou de chave pública, um problema central é a correta distribuição das chaves públicas das entidades. Essa distribuição é feita, usualmente, por meio de certificados digitais [18], que são credenciais emitidas e assinadas digitalmente por entidades confiáveis. Um certificado contém, geralmente, uma chave pública, informação necessária sobre seu dono e metadados necessários ao seu processamento (para maiores detalhes, ver Seção 3.2). Logo, quando um usuário necessita utilizar a chave pública de outro, o segundo deve prover o seu certificado ao primeiro, que deve validá-lo. O arcabouço para gerenciamento do ciclo de vida dos certificados, isto é, emissão, renovação, revogação e principalmente validação, é usualmente uma hierarquia de terceiras partes confiáveis, ou autoridades certificadoras (ACs), cujos nós mais inferiores correspondem aos usuários finais dos certificados. A esse arcabouço organizacional que inclui software e hardware dá-se o nome infraestrutura de chaves públicas (ICP) ou, em inglês, *public-key infrastructure* (PKI).

O processo de validação de um certificado consiste em conferir sua autenticidade, processar seus metadados e determinar seu estado (se foi revogado ou não). Na Seção 3.3, aborda-se com maior profundidade o problema da validação de certificados. Por hora, basta dizer que tal processo é custoso, pois envolve operações criptográficas, principalmente de verificação de assinaturas, que são consideradas computacionalmente custosas. Esse custo se torna mais crítico quando se consideram ICPs complexas ou ainda um aglomerado de ICPs interligadas, pois, nesse caso, geralmente, a obtenção de uma chave pública exige que vários certificados sejam validados ao longo do que se denomina caminho de certificação (ver Seção 3.4).

Vários esquemas foram propostos para reduzir o custo de validação dos certificados, entre eles NOVOMODO [26], CRT [17], EFFECT [14] e certificados efêmeros [31]. Embora esses mecanismos tenham tornado mais eficiente o processo de validação de certificados digitais, eles ainda necessitam de um número de verificações de assinaturas digitais igual ao número de certificados no caminho de certificação, k.

Por outro lado, Levi et al [20] propuseram a ICPA, baseada em certificados aninhados

(do inglês, *nested certificate*), que são certificados emitidos para outros certificados, os certificados-alvo (*subject certificate*). A ICPA permite que a validação do caminho de certificação possa ser realizada com apenas uma operação de verificação de assinatura digital e $k-1$ operações de resumo (para um caminho de certificação com k certificados). Ou seja, há significativa redução do custo computacional de se validar o caminho de certificação, pois as operações de resumo (também conhecidas como operações de *hash*) têm custo muito menor do que a verificação de assinaturas digitais [26]. O ponto negativo do esquema é o número de certificados aninhados emitidos, o que impõe uma sobrecarga significativa à ICPA, especialmente às ACs, tornando o esquema custoso para ICPAs de grande porte.

Objetivos

Dessa forma, o presente trabalho segue uma linha mestra que é propor melhorarias para o processo de validação de certificados digitais. Para isso, inicialmente faz-se uma revisão bibliográfica extensiva dos mecanismos de validação de certificados digitais propostos na literatura, analisando-se seus custos de processamento e de transmissão, principalmente no que tange ao verificador (ver Seção 3.5). A partir dos resultados obtidos, propõem-se alterações que tornem o processo de validação dos certificados digitais mais eficiente. Mais precisamente, será apresentado um novo modelo de construção para a ICPA, ICPAm, em adição aos dois propostos por Levi et al [20], que reduz os custos de validação dos certificados digitais em relação aos mecanismos tradicionais, mas não sobrecarregue os outros elementos da estrutura excessivamente, em especial as ACs.

Contribuições

O presente trabalho traz duas contribuições principais:

- a primeira é fazer uma extensiva revisão bibliográfica sobre mecanismos de validação de certificados digitais, principalmente no que se refere aos seus custos de transmissão e processamento ao se validar um caminho de certificação;
- a segunda contribuição é propor uma nova política para emissão de certificados aninhados, de forma que a ICPA resultante (denominada ICPAm) seja mais escalável do que a ICPA, ou seja, o número de usuários finais não comprometa o desempenho da ICPAm.

Organização da dissertação

Inicialmente, no Capítulo 2, apresentam-se os conceitos básicos de Criptografia, como primitivas simétricas, assimétricas, funções de *hash*, etc. Nesse capítulo também introduz-se a notação que será utilizada no decorrer deste trabalho.

No Capítulo 3 discutem-se o problema da validação de certificados digitais e as infraestruturas de chaves públicas, arcabouço que suporta a validação dos certificados. O capítulo termina com uma descrição dos custos de validação dos certificados, principalmente os de transmissão e os de processamento.

No Capítulo 4 apresentam-se os principais mecanismos de validação de certificados digitais e os respectivos custos de processamento e transmissão associados à validação dos certificados em cada mecanismo.

No Capítulo 5 é proposta uma nova política para emissão de certificados aninhados, que resulta em maior escalabilidade das ICPAs.

Finalmente, o Capítulo 6 contém as conclusões e as sugestões para trabalhos futuros.

Capítulo 2

Conceitos de Criptografia

Criptografia (do grego kriptos = escondido, oculto; grapho = escrita) é definida historicamente como sendo a arte ou ciência de escrever em cifra ou em código, de forma a permitir que apenas o destinatário da mensagem a decodifique e a compreenda. A decodificação geralmente requer o uso de uma chave, uma informação secreta, disponível apenas ao destinatário.

A Criptografia é utilizada desde a antiguidade na troca de mensagens secretas, principalmente relativas aos assuntos militares e diplomáticos. Um dos exemplos mais conhecidos é a Cifra de César, utilizada pelo imperador para enviar mensagens secretas aos seus generais. A Criptografia também foi muito utilizada na segunda guerra mundial.

Na segunda metade do século XX, com o surgimento dos computadores e da Internet, a Criptografia começou a ganhar campo no cotidiano das pessoas, sendo hoje vastamente utilizada, por exemplo, em transações comerciais, bancárias, governamentais, etc., principalmente nas realizadas pela Internet. Também na segunda metade do século XX, surgiram novas técnicas criptográficas, possibilitando, além do serviço de confidencialidade (segredo), a utilização de outros serviços, como autenticação, integridade e não repúdio.

A **confidencialidade**, como foi dito, é o serviço que garante o sigilo da informação, exceto àqueles que estão autorizados a vê-la. Ou seja, dado que Bob enviou uma mensagem para Alice, através de um canal que provê confidencialidade, seja ele físico (fio) ou lógico (através do ciframento/deciframento das informações), somente Alice (além de Bob) está apta para ver o conteúdo da mensagem.

A **integridade** é o serviço que garante que somente pessoas autorizadas sejam capazes de modificar a informação. Qualquer mudança não autorizada é detectada pelo receptor. Por exemplo, se Bob envia uma mensagem para Alice através de um canal que provê o serviço de integridade, então Alice é capaz de detectar qualquer modificação, acidental ou não, que tenha sido feita na mensagem de Bob.

A **autenticação** é o serviço que permite a uma entidade estabelecer uma propriedade reivindicada por outra [21]. Pode-se pensar em autenticação sobre duas formas: **autenticação de entidade** e **autenticação de origem de dados**. No primeiro caso valida-se a identidade de uma entidade, enquanto no segundo valida-se a reivindicação de que a mensagem foi emitida por uma determinada entidade.

O serviço de **não repúdio** garante que uma entidade não poderá negar uma ação

que tenha praticado previamente. Se há uma disputa entre duas entidades sobre uma determinada ação, uma terceira entidade, que possui a confiança das duas primeiras, deve interferir para resolver a disputa.

A partir dos conceitos acima, pode-se fornecer uma definição mais moderna para **Criptografia**: é o estudo das técnicas matemáticas relacionadas aos aspectos de segurança da informação como confidencialidade, integridade, autenticação e não repúdio [22].

2.1 Primitivas criptográficas

Podem-se dividir as primitivas criptográficas em três grupos: primitivas sem chaves, primitivas de chave simétrica e primitivas de chave assimétrica [22]. As próximas seções contêm uma descrição breve desses grupos e a respectiva notação utilizada.

2.1.1 Primitivas sem chave

As já mencionadas **funções de resumo criptográfico** (ou resumo simplesmente, ou *hash*) são uma das representantes desse conjunto. Uma função de resumo $\mathrm{H}(x)$ é uma função determinística que mapeia uma sequência de bits x de tamanho arbitrário numa sequência de tamanho fixo y, denominada resumo ou *hash* [21].

Uma função de resumo deve possuir as seguintes propriedades [22]:

- compressão: para uma entrada de tamanho arbitrário, gera-se uma saída de tamanho fixo e pré-determinado;
- fácil computação: a computação da função de resumo sobre uma entrada é computacionalmente eficiente;
- resistência à inversão (função de mão-única): a função não pode ser facilmente invertida, ou seja, dado y ($y = \mathrm{H}(x)$), é inviável computacionalmente encontrar x;
- resistência à segunda inversão (resistência fraca a colisões): é inviável computacionalmente, dado $y = \mathrm{H}(x)$, encontrar $x' \neq x$ tal que $y = \mathrm{H}(x')$;
- resistência a colisões (resistência forte a colisões): é inviável computacionalmente encontrar x e x', $x \neq x'$, tal que $\mathrm{H}(x) = \mathrm{H}(x')$.

As funções de resumo são de grande importância para a Criptografia. Elas são comumente usadas associadas a assinaturas digitais, permitindo que se assine o resumo (de tamanho fixo e geralmente muito menor do que a mensagem) em vez da mensagem propriamente dita, garantindo o mesmo nível de segurança.

O principal algoritmo de resumo em uso é o *secure hash algorithm* (SHA-1) [1].

2.1.2 Primitivas de chaves secretas ou simétricas

As primitivas de chaves secretas são as que utilizam a mesma chave, ou chaves que podem ser facilmente deduzidas uma a partir da outra, para cifrar e decifrar mensagens; daí o

adjetivo simétricas. Entre os principais representantes dessa classe estão o AES [4], o DES [2] (obsoleto) e o 3-DES (*tiple* DES) [2].

As principais características dessas primitivas são:

- a troca de chaves deve ser feita através de um canal que garanta autenticidade e confidencialidade;
- são computacionalmente mais eficientes quando comparadas às primitivas assimétricas, descritas a seguir;
- utilizam chaves menores do que as primitivas assimétricas. Atualmente, chaves de 128 bits são consideradas seguras;
- para um ambiente com x entidades, para que todas possam se comunicar aos pares de forma segura, é necessário que cada par de entidade compartilhe uma chave distinta, ou seja, é necessário gerenciar o ciclo de vida de até $\frac{x(x-1)}{2}$ chaves distintas, o que compromete a escalabilidade de tais primitivas em ambientes com muitos usuários.

2.1.3 Primitivas de chaves públicas ou assimétricas

Os sistemas criptográficos assimétricos utilizam duas chaves distintas, uma das quais é mantida em segredo pela entidade titular do par e a outra é tornada pública. A primeira é conhecida como chave privada enquanto a segunda é conhecida como chave pública. Essas chaves são construídas de forma que o que é cifrado com uma chave pública só pode ser decifrado com a chave privada correspondente. No entanto, não é possível deduzir a chave privada da chave pública, a não ser através da solução de problemas considerados difíceis, como o problema da fatoração de números primos e o problema do logaritmo discreto. Maiores detalhes para esses problemas podem ser encontrados em Mao [21], Menezes et al [22] e Stinson [33].

Entre os principais criptossistemas assimétricos estão o RSA [32, 6] e o DSA [3]. O primeiro é baseado na dificuldade de fatorar número primos enquanto que o segundo é baseado no problema do logaritmo discreto.

As principais características das primitivas assimétricas são:

- para a troca de chaves é necessário apenas um canal que provê autenticidade (apenas a chave pública é transmitida). Essa característica é significativa, pois permite a simplificação do processo de distribuição de chaves assimétricas quando comparado ao de chaves simétricas, que além da autenticidade também exige confidencialidade da chave;
- as primitivas assimétricas proveem a propriedade do não repúdio, pois somente a entidade titular do par de chaves possui a chave privada (ver assinatura digital adiante);
- são menos eficientes do que as primitivas simétricas, pois geralmente utilizam operações com chaves muito grandes, da ordem de milhares de bits;

- para enviar uma mensagem cifrada para uma determinada entidade, todas as demais entidades usam a mesma chave pública, que faz par com a chave privada da entidade para a qual se quer enviar a mensagem. Logo, para um ambiente com x entidades, é necessário apenas uma chave pública por entidade, ou seja, x chaves públicas no total devem ser gerenciadas, permitindo melhor escalabilidade em ambientes com muitos usuários.

Assinaturas digitais

De forma similar as assinaturas cursivas tradicionais, assinaturas digitais permitem identificar, com alta probabilidade, o autor de uma mensagem assinada. Diferentemente das assinaturas cursivas, porém, assinaturas digitais dependem da mensagem sendo assinada, além do autor da mensagem. Isso significa que se a mensagem for alterada, a assinatura não é mais válida. Em outras palavras, através da assinatura digital é possível garantir, além autenticidade, a integridade da mensagem.

Mais especificamente, assinaturas digitais são constituídas de um par de procedimentos $\text{SIGN}_{d_A}(x)$ e $\text{VER}_{e_A}(s, x)$ tais que: (i) d_A e e_A são as chaves privada e pública da entidade A; (ii) $\text{SIGN}_{d_A}(x)$ é função que retorna uma cadeia de bits s, chamada de assinatura de A em x; e (iii) $\text{VER}_{e_A}(s, x)$ é um predicado que retorna "verdadeiro" se, e somente se, $s = \text{SIGN}_{d_A}(x)$. Assim a assinatura digital é uma prova de que A confeccionou a assinatura s usando para isso x e sua chave privada d_A, o que impossibilita que A repudie ter assinado x.

Pelo que foi explanado, é possível perceber outra característica peculiar às assinaturas digitais: elas são baseadas na posse da chave privada. Se Bob também conhece a chave privada de Alice, então não é possível determinar quem gerou uma determinada assinatura. Esse paradigma é diferente das assinaturas cursivas, em que a assinatura depende das características do indivíduo e não de algo que somente ele possui.

Tal característica tem uma implicação de ordem prática: para que a propriedade de não repúdio seja alcançada, é necessário utilizar assinaturas digitais em conjunto com um selo cronológico (*secure timestamp*), ou seja, uma indicação de tempo assinada digitalmente por uma TTP. Caso não houvesse o selo cronológico, para negar uma assinatura, bastaria uma entidade alegar o comprometimento da sua chave privada. Na falta da indicação de tempo, não haveria como distinguir, como explicado no parágrafo anterior, quem assinou a mensagem.

Capítulo 3

Validação de certificados digitais

Este capítulo aborda a validação de certificados digitais, mais precisamente, o problema de validar tais certificados, as infraestruturas de chaves públicas e a definição dos custos associados à validação dos certificados digitais.

3.1 Distribuição de chaves criptográficas

Um dos mais importantes alicerces da Criptografia e dos serviços baseados nela é a distribuição de chaves criptográficas. Serviços como confidencialidade, integridade, autenticidade, não repúdio, etc. são possíveis apenas quando se faz certas suposições sobre as chaves envolvidas. Por exemplo, quando se diz que uma mensagem satisfaz o requisito de confidencialidade, utilizando a técnica de ciframento, está implícito que apenas os usuários autorizados possuem a chave para decifrá-la. Caso essa suposição não seja verdadeira, não há como garantir tal propriedade. O mesmo ocorre quando se utiliza assinaturas digitais: o conceito de assinatura digital só tem efeito quando se assume que o verificador tem a chave pública correta do autor da assinatura e que esse é o único a possuir a respectiva chave privada.

A distribuição de chaves criptográficas também é um dos problemas mais complexos da Criptografia moderna. Quando se considera uma chave simétrica, o canal a ser utilizado para a sua distribuição deve prover tanto confidencialidade quanto autenticidade da chave. O estabelecimento de tal canal pode se tornar uma tarefa difícil, principalmente em ambientes em que as partes comunicantes estão geograficamente distantes. Além disso, quando se utiliza chaves simétricas, cada entidade deve manter uma chave, às vezes diferente, para cada entidade com a qual deseja manter comunicação. Essas características tornam a distribuição de chaves simétricas complicada e pouco escalável. Em uma ICP com n entidades, o número de chaves a ser gerenciado é $n\frac{n-1}{2}$, casos todas as entidades interajam entre si.

Por outro lado, a distribuição de chaves públicas é mais simples. Como a chave a ser distribuída é pública, não é necessário utilizar um canal que garanta a confidencialidade dela. Além disso, cada entidade deve manter apenas um par de chaves, pois a mesma chave pública é utilizada para interagir com todas as outras entidades, seja para cifrar mensagens ou conferir assinaturas digitais. Isso torna a distribuição de chaves públicas

mais escalável do que a distribuição de chaves simétricas, uma vez que o número de pares de chaves a ser gerenciado em uma ICP com n entidades, interagindo entre si, é igual a n.

Embora à primeira vista a distribuição de chaves públicas pareça ser trivial, ainda é necessário garantir a autenticidade da chave. Caso contrário, numa comunicação entre duas partes, um intruso hostil poderia substituir a chave pública de uma delas pela sua, tornando-o apto a ler mensagens destinadas à parte em questão ou até mesmo se passar por uma delas perante a outra. Por exemplo, suponha que Bob vai enviar uma mensagem secreta para Alice (cuja chave pública é e). Bob, através de um canal sem garantia de autenticidade, obtém a chave e', fornecida pelo intruso como se fosse a chave de Alice. Bob não tem como identificar que a chave foi mudada. Ele cifra a mensagem com e' e a envia para Alice. O intruso agora está apto a decifrar a mensagem de Bob para Alice, pois possui a chave privada referente à chave pública e'. Para que não seja percebido, ele também envia a mensagem para Alice, cifrada com a chave e. Esse ataque é conhecido como ataque do homem do meio (*man-in-the-middle*) [21].

Logo, há a necessidade de se garantir a autenticidade da chave pública, de forma que quem a receba tenha como verificar que ela realmente pertence à entidade que se diz dona dela. Ou seja, o problema de distribuição de chaves públicas se reduz a um problema de autenticação [21].

Uma classe de mecanismos de autenticação que têm sido largamente utilizada é a emissão de certificados digitais por terceiras partes confiáveis (TPCs) ou, em inglês, *trusted third parties* (TTPs). O princípio de funcionamento desses mecanismos é a TTP validar uma associação entre a chave pública e uma propriedade dela, por exemplo, a identidade da entidade que possui a chave privada correspondente, através da emissão de um certificado digital (ver Seção 3.2 para maiores detalhes). Entre esses mecanismos estão o *Pretty Good Privacy* (PGP) [7] e o X.509 [15].

Especificamente para o padrão X.509, a obtenção de uma chave pública de uma entidade consiste em obter o certificado daquela entidade e validá-lo. Pode-se dizer, a grosso modo, que nesse caso, o problema da distribuição de chaves públicas restringe-se ao problema de validar um certificado. A Seção 3.2 define e caracteriza o certificados digitais e a Seção 3.3 apresenta o problema da validação dos certificados digitais.

Para finalizar, o leitor deve observar que uma vez que duas entidades tenham trocado suas chaves públicas, elas podem estabelecer chaves simétricas de forma direta e simples. Utilizando-se algoritmos de chave pública, é possível cifrar (confidencialidade) e assinar (autenticidade) uma chave simétrica e transmiti-la à outra parte interessada. Esse procedimento necessita do conhecimento mútuo das chaves públicas das entidades participantes. O destinatário deve conhecer a chave pública do emissor para verificar a assinatura e o emissor deve conhecer a chave pública do destinatário para cifrar a mensagem.

3.2 Certificados digitais

Certificados digitais são credencias eletrônicas, compostos de um conteúdo ($Cont_c$) e uma assinatura digital (Sig_c), gerada por uma TTP sobre o resumo criptográfico de tal

conteúdo. A Figura 3.1 mostra graficamente a estrutura de um certificado. A assinatura digital é necessária para garantir a autenticidade do conteúdo do certificado. O conteúdo é a concatenação de metadados (como versão, emissor, número de série e data de validade ou período) e uma associação que depende da categoria do certificado.

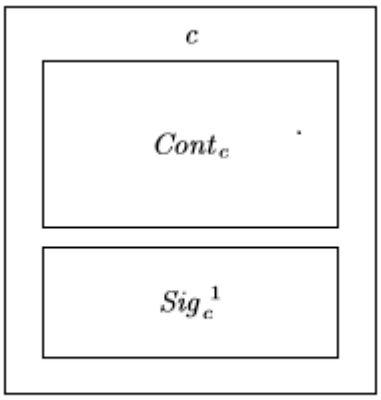


Figura 3.1: Certificado digital

Existem três categorias de certificados: **certificados de identidade** (*identity certificates*), **certificados de autorização** (*authority certificates*) e **certificados de atributos** (*attribute certificates*).

Os certificados de identidade estabelecem uma associação entre uma chave pública e a identidade do seu titular, que consiste em informações que tornam possível identificar o titular unicamente. O padrão X.509, cujos certificados são os principais representantes dessa categoria, propõem que seja utilizado como identidade um nome globalmente único (*distinguished name*).

Os certificados de autorização definem uma associação entre a chave pública e uma autorização dada ao portador da chave privada correspondente à chave pública para realizar uma determinada ação. Os principais representantes dessa classe são os certificados definidos pelo *Simple Infrastructure Public Key* (SPKI/SDSI) [12].

Finalmente, os certificados de atributo são aqueles que estabelecem uma associação entre um atributo e a identidade da entidade. Observe que quando o atributo é uma autorização, combinando o certificado de atributo e o respectivo certificado de identidade, obtém-se uma associação entre a autorização e a chave pública.

3.3 O problema da validação de certificados digitais

O problema da validação de certificados digitais consiste em verificar que, em um determinado instante de tempo, a associação estabelecida pelo certificado é válida. Para tal é necessário:

- **verificação de autenticidade**: consiste em determinar se o certificado realmente foi emitido por uma entidade confiável e se o seu conteúdo não foi alterado, seja

de forma acidental ou induzida por um intruso. Isso impede, por exemplo, que um intruso possa substituir a chave pública legítima da entidade para a qual o certificado foi emitido pela dele e, consequentemente, esteja apto a ser passar por tal entidade, seja assinando documentos ou decifrando mensagens;

- **verificação de estado**: ao emitir um certificado, o emissor determina o prazo de validade do mesmo, isto é, o período de tempo em que o certificado pode ser utilizado, sob condições normais. Consequentemente, o emissor também determina o período em que a chave pública pode ser utilizada. Após esse prazo, o certificado perde sua validade (expira) e a chave pública não deve mais ser utilizada, exceto para eventos que tenham ocorrido no passado, durante o período de validade do certificado. A chave pública pode voltar a ser utilizada se outro certificado for emitido para ela.

  No entanto, no decorrer do prazo de validade de um certificado, podem ocorrer eventos, fora do controle do emissor, que impliquem na invalidação da associação estabelecida pelo certificado antes do mesmo expirar. Nesse caso, o certificado deve ser revogado. Deve-se deixar bem clara a distinção entre expiração e revogação. Embora em ambos os casos a associação determinada pelo certificado não é mais válida, no primeiro caso, isso ocorre sob controle do emissor, num instante de tempo determinado e sua ocorrência pode ser determinada através da observação do certificado. No segundo, isso ocorre a qualquer momento, fora do controle do emissor e essa ocorrência não pode ser determinada pela simples observação do certificado.

  Dadas as características da revogação, sempre que o verificador for utilizar o certificado, ele deve inquirir o emissor do mesmo (ou a entidade que recebeu a delegação do emissor) sobre o estado do certificado, isto é, se foi ou não revogado. Os métodos que possibilitam tal operação recebem o nome de mecanismos de verificação de informação de revogação (ver Seção 4.1). A informação propriamente dita, disponibilizada pelo emissor, denomina-se **informação de revogação**. O **servidor de informação de revogação** é a entidade responsável por disponibilizar tais informações para os verificadores;

- **processamento**: geralmente, o certificado contém meta-informação que deve ser processada para a correta validação do mesmo. Por exemplo, o certificado pode conter políticas relativas à emissão/verificação do certificado, restrições de uso, prazo de validade, etc. Uma vez que tais características não estão diretamente relacionadas à criptografia, mas sim a questões administrativas e gerenciais, elas não serão mais tratadas nesse trabalho. Em relação ao modelo X.509, essa questão é abordada por Housley et al [15], tanto no que tange às extensões acrescidas aos certificados quanto ao algoritmo utilizado no processamento.

Para tornar mais clara a ideia, considere o exemplo em que a entidade A tenha emitido o certificado c; o verificador V possua a chave pública de A e confie em A; ainda, que o verificador possua o certificado c e a respectiva informação de revogação ir_c. Nesse caso, os procedimentos para validar c são:

- a verificação da sua autenticidade, efetuada através da conferência da assinatura da AC emissora contida em c;
- a verificação do seu estado, feita através da consulta de ir_c, como descrito na Seção 4.1;
- o seu processamento, através da análise de seus metadados.

O exemplo acima é uma visão simplificada do problema e de sua solução. Especificamente:

- existe uma informação de revogação disponível, ir_c. Num ambiente real, essa informação deve ser obtida através de um mecanismo específico, tal como LCRs [15], OCSP [27], NOVOMODO [26], etc. Esses mecanismos serão estudados na Seção 4.1. As informações relativas ao mecanismo de revogação são incluídas nos certificados, geralmente através de extensões [7, 15];
- são satisfeitas as condições "o verificador confia em A" e "o verificador possui a chave pública de A", ponto no qual está a principal simplificação feita no exemplo anterior. O estabelecimento das relações de confiança e a obtenção das chaves públicas das entidades emissoras são complexas. Elas serão abordadas na Seção 3.4, onde será discutido o conceito de infraestrutura de chaves públicas (ICPs).

3.4 Infra-estruturas de chaves públicas

No exemplo anterior, as pré-condições eram: o verificador confia na entidade que emitiu o certificado e possui a chave pública dela. Satisfazer essas condições não é simples, principalmente em ambientes reais. Um dos primeiros problemas é como o verificador determina se uma entidade é confiável. Por confiável entende-se que o verificador acredita que as informações geradas pela entidade (e assinadas por ela) são verdadeiras. Uma vez que o verificador confia na entidade, ele não tem como avaliar se tais informações são verdadeiras ou falsas. Ele simplesmente supõe que são verdadeiras. Por isso, essas entidades são conhecidas como **autoridades certificadoras** ou ACs. Especificamente, a autoridade certificadora com a qual o cliente estabelece confiança diretamente também é conhecida como **AC âncora** ou **AC de confiança**. O verificador pode ter uma ou mais ACs de confiança.

O processo pelo qual o cliente elege sua AC âncora envolve tanto critérios técnicos como não técnicos. Entende-se como técnicos os critérios relacionados aos aspectos criptográficos e gerenciais da infraestrutura, como algoritmos utilizados, cuidados com a manutenção da chave privada da AC, etc. Por critérios não técnicos entende-se aqueles que envolvem aspectos político-sócio-econômicos, por exemplo, custos financeiros, a reputação da instituição (um dos mais importantes), os interesses político-econômicos dos controladores da AC, a competência (se possui competência legal atribuída por autoridade competente, como no caso da ICP-Brasil [5]), etc.

Uma vez que o cliente elege sua AC âncora, o próximo passo é obter uma cópia autêntica da chave pública dela. Observe que nesse caso, não se pode utilizar um certificado

ou se incorreria num problema recursivo. Logo, para a distribuição dessa chave é preciso utilizar um mecanismo tradicional, por exemplo, o usuário vai à sede da AC e obtém uma mídia com a chave pública da mesma (certificado auto assinado). Outra forma seria publicar a chave em um documento de grande circulação, disponibilizar a chave eletronicamente e solicitar ao usuário que a compare com a impressa (esse mecanismo é utilizado pela ICP Brasil para distribuir a chave da AC raiz).

Para o exemplo anterior (Seção 3.3), em que a autoridade de confiança do verificador é a autoridade emissora do certificado a ser verificado, o processo descrito é uma solução razoável. No entanto, num ambiente real, o certificado a ser verificado pode ter sido emitido por uma AC que não a de confiança do verificador. Uma solução óbvia para esse caso seria repetir o processo acima e tornar a AC em questão uma AC de confiança do verificador. Embora essa solução seja possível, ela apresenta algumas limitações: primeiro, antes de confiar numa AC, ela deve ser analisada tanto do ponto de vista técnico como não técnico, habilidade que poucos usuários possuem; segundo, a obtenção da chave pública da AC em questão é um processo que pode ser complexo e demorado. Atribuir tais funções ao usuário final para cada nova AC cujo certificado ele precisa verificar, é condenar a utilização dos certificados digitais à morte prematura.

A solução adotada foi o usuário permitir que sua AC âncora possa estender a confiança que ele deposita nela para outras ACs. Isso significa que o usuário passa a confiar em outras ACs através de sua AC âncora. Essa transitividade de confiança é estabelecida através da emissão de um certificado da AC de confiança para a outra AC, o que denominou-se **certificação cruzada**.

Para tornar a ideia mais clara, considere o exemplo da Figura 3.2. A AC A_1 emite um certificado para a AC A_2. Esse certificado é visto pelo verificador que tem A_1 como AC de confiança, por exemplo, u_1, com o seguinte significado: A_2 pode ser utilizada para validar os certificados de u_3 e u_4 e a chave pública dela é a contida neste certificado (c_1).

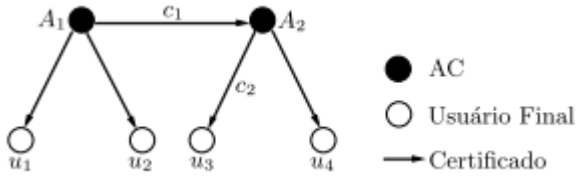


Figura 3.2: Exemplo de uma ICP simples

O usuário verificador, primeiro valida o certificado c_1, obtendo uma chave válida de A_2. Em seguida, valida o certificado c_2 do usuário u_3. Uma vez que c_2 tenha sido validado, a chave de u_3 pode ser utilizada.

Essa sequência de certificados a serem validados, cujo primeiro pertence à AC âncora do verificador e o último ao usuário do qual se deseja obter a chave pública, é denominada **caminho de certificação** (CC). Num caminho de certificação podem existir várias ACs intermediárias, o que torna possível caminhos de qualquer tamanho, em teoria. Na prática, o número se mantém pequeno, dificilmente excedendo 5 certificados.

A partir do exemplo acima, observa-se que para usar uma chave (a de u_3) é necessária a validação de todos os certificados do caminho de certificação existente entre a AC de

confiança do verificador e o usuário cuja chave se quer obter, ou seja, é necessário validar o caminho de certificação. Isso significa validar individualmente cada um dos certificados que compõem o caminho e também garantir que: (i) o primeiro certificado do caminho de certificação é assinado pela AC de confiança do verificador; (ii) o último certificado pertence ao usuário do qual se deseja obter a chave pública; e (iii) para todo certificado x no caminho de certificação, o certificado que segue x tem como emissor o titular de x.

A esse arcabouço, composto por software, hardware, procedimentos, entidades (ACs, usuários finais, etc.), contratos, etc., que suporta a distribuição de chaves públicas de forma autêntica e a transitividade de confiança, denomina-se infraestrutura de chaves públicas ou ICP. A Figura 3.2 é o exemplo de uma ICP composta por duas autoridades certificadoras e 4 usuários finais.

Em ambientes reais, as relações e serviços exigidos são mais complexos, resultando em ICPs mais complexas. A Figura 3.3 é o exemplo de uma ICP mais complexa, com várias ACs e vários usuários finais.

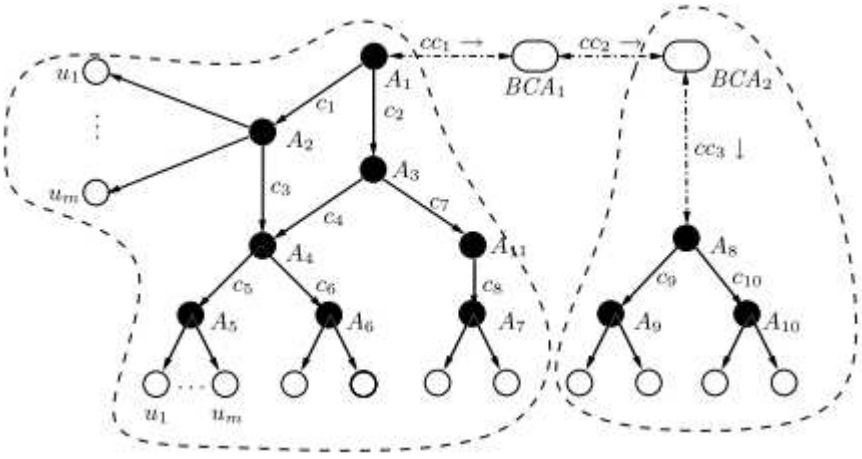


Figura 3.3: Exemplo de uma ICP Complexa

Foi dito anteriormente que quando uma AC emite certificado para outra AC, tal emissão é definida como certificação cruzada [7]. Quando a certificação ocorre entre ACs dentro de um mesmo domínio administrativo, diz-se que ocorre certificação cruzada intradomínio. Quando a certificação ocorre entre ACs de domínios administrativos diferentes diz-se que ocorre certificação cruzada inter-domínio.

Na Figura 3.3, a AC A_1 estabelece certificação cruzada intradomínio com as ACs A_2 e A_3 e certificação cruzada inter-domínio com BCA_1. Ainda nota-se que a certificação cruzada pode ser unidirecional (por exemplo entre A_1 e A_3) ou bidirecional (entre A_1 e BCA_1).

Existem várias abordagens para construção de ICPs, cada uma com suas peculiaridades. Entre as mais conhecidas estão as baseadas no padrão X.509, a SPKI e o PGP. A seguir, faz-se uma breve discussão de cada uma.

X.509

O modelo X.509 é um padrão do ITU e faz parte do padrão X.500 e define conceitos gerais para autenticação baseada em chaves públicas, inclusive o formato dos certificados. O grupo de trabalho PKIX especializou tal proposta para tornar possível a interoperabilidade de implementações para a Internet, publicando várias RFCs, uma das quais é a RFC 3280 [15], que trata do formato dos certificados para a Internet.

O padrão X.509 não define uma topologia específica para ICPs, mas determina características gerais que são:

- fortemente centralizada e hierárquica;
- há distinção clara entre ACs e usuários finais. As primeiras são entidades confiáveis e são responsáveis pela emissão de certificados. Os usuários finais não podem emitir certificados;
- uso de certificados de identidade, sendo a entidade identificada por um nome que deve ser globalmente único. Também suporta o uso de certificados de atributos.

Pretty Good Privacy - PGP

O PGP foi proposto por Phill Zimmermann com objetivo de definir uma infra-estrutura onde os usuários fossem o centro das relações de confiança, permitindo que esses possuíssem mais poder de escolher suas próprias políticas. As principais características do PGP são:

- não há uma distinção entre AC e usuário final, ou seja, qualquer usuário pode se comportar como uma AC, emitindo certificados . Além disso, várias ACs/usuários independentes (não necessariamente confiáveis) podem (e devem) assinar um mesmo certificado. O princípio de funcionamento do PGP é que tomando-se várias dessas assinaturas, pode-se confiar no certificado, pois nem todas as entidades são corruptas. Esse modelo é conhecido com rede de confiança (*web of trust*).
- o usuário escolhe em quem confiar, estabelecendo níveis de confiança em outros usuários;
- descentralização e ausência de hierarquia, já que cada usuário emite seu próprio certificado e escolhe em quem confiar;
- do mesmo modo que o modelo X.509, o PGP também utiliza certificados de identidade. Em versões mais recentes, o PGP também é compatível com certificados X.509. O PGP também identifica os usuários através de nomes globalmente únicos;
- por causa da relativa liberdade do usuário para tomar decisões, o PGP pode não ser viável para ambientes com usuários leigos.

***Simple Public-key Infrastructure* - SPKI**

O SPKI [12] surgiu como uma alternativa ao X.509, que na visão do grupo de trabalho SPKI é muito complexo. Logo, a principal reivindicação do SPKI é ser um modelo mais simples do que o X.509. A seguir as principais características do SPKI:

- há distinção entre AC e usuário final, de forma semelhante ao padrão X.509;
- utiliza certificados de autorização;
- uso de nomes locais ao invés de nomes globais e hierárquicos como no X.509. Nomes locais são os utilizados no quotidiano para identificar a entidade no seu ambiente, por exemplo, o próprio nome da pessoa, apelido, identificação atribuída pela corporação, etc.

3.5 Custos de validação dos certificados digitais

Até o momento, discutiu-se o problema da validação sob a ótica estrutural e gerencial. Nesta seção, analisa-se o problema sob o ponto de vista dos custos de validação dos certificados.

Entende-se aqui por custo a noção clássica de complexidade de algoritmos que mede o esforço computacional em função do tamanho da instância processada, expressa em unidades relevantes ao processo. No caso de operações com inteiros muito grandes, como é o caso de algoritmos assimétricos, foco de nossa análise, operações aritméticas, espaço de memória ocupado e banda de transmissão são unidades relevantes. No caso de dispositivos móveis, dependentes de fontes de alimentação limitadas, energia despendida nas operações aritméticas e na transmissão e recepção de dados é outra unidade importante.

Neste trabalho, analisa-se o custo sob duas óticas: uma do verificador e outra do ASR, que compreende os demais elementos da infraestrutura de chaves públicas envolvidos (AC, repositório de certificados e servidor de informações de revogação). Para efeitos de cálculos, não se faz distinção entre as operações realizas pelo ARS, tratando-o como um bloco. A Figura 3.4 mostra o que foi dito.

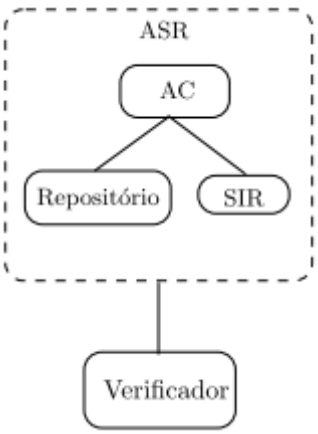


Figura 3.4: Modelo para cálculo de custo de validação de certificados digitais

O custo computacional de validação dos certificados do verificador C_V pode ser expresso pela soma

$$C_V = C_E + C_C + C_R, \tag{3.1}$$

em que:

- C_E é o custo do verificador para extrair e processar as informações contidas nos certificados e nas informações de revogação, tais como atributos do titular e do emissor, políticas de uso, data de validade, etc.;
- C_C é o custo de operações criptográficas do verificador para conferir os certificados e as informações de revogação ao longo do caminho de certificação;
- C_R é o custo de transmissão ou comunicação do verificador para obter os certificados e as informações de revogação.

Por outro lado, para gerar e disponibilizar aos verificadores os dados necessários à validação dos certificados, o ASR tem um custo C_D que pode ser expresso pela soma

$$C_D = C_M + C_A + C_T, \tag{3.2}$$

em que:

- C_M é o custo do ASR de montar os certificados e as informações de revogação, ou seja, o custo para criar as estruturas de dados que serão assinadas posteriormente, dando origem aos certificados e informações de revogação;
- C_A é o custo de operações criptográficas do ASR para criar os certificados e as informações de revogação;
- C_T é o custo de transmissão ou comunicação do ASR para disponibilizar as informações de revogação.

Neste trabalho, os custos C_E e C_M não serão considerado nos cálculos de eficiência do processo de validação, pois o interesse é apenas nos custos diretamente relacionados ao uso de criptografia.

Os custos C_C e C_A normalmente consistem de operações criptográficas, principalmente operações assimétricas, consideradas custosas já que envolvem até centenas de operações aritméticas entre números inteiros da ordem de milhares de bits. Por isso, dá-se atenção especial para estes custos, tentando torná-los o menor possível. Em especial, tem-se interesse em reduzir o custo do verificador, C_C, sem provocar aumentos significativos nos demais custos.

O custo de transmissão compreende apenas os dados resultantes da utilização de algoritmos criptográficos (em especial a assinatura digital computada). Informações contidas nos certificados (chave pública, validade, emissor, titular, etc.) e nas informações de revogação (estado, validade, emissor, etc.) não serão consideradas.

No próximo capítulo, introduzem-se os principais mecanismos de validação conhecidos na literatura e seus respectivos custos.

Capítulo 4

Mecanismos de validação de certificados digitais

A validação de certificados digitais é um assunto de grande interesse. Surgiram vários trabalhos na literatura com o intuito de melhorar o desempenho dos mecanismos de validação de certificados [8, 14, 17, 20, 26, 28], principalmente no que tange ao processo de revogação. Para analisar tais mecanismos, eles serão divididos em duas classes: mecanismos de verificação de informação de revogação (Seção 4.1) e mecanismos integrados (Seção 4.2). Na Seção 4.3 é feita uma análise dos custos de transmissão e processamento envolvidos nos mecanismos descritos.

4.1 Mecanismo de verificação de informação de revogação

Os mecanismos desta classe abordam apenas a questão de determinar se o certificado foi ou não revogado. Isso quer dizer que eles não tratam da verificação de integridade e autenticidade do certificado, que deve ser feita pela verificação da assinatura contida no mesmo. Entre esses mecanismos, os seguintes se destacam: LCR [15], OCSP [27], NOVOMODO [26], CRT [17] e 23CRT [28].

4.1.1 LCRs

Os primeiros mecanismos propostos para disponibilizar informações de revogação foram os baseados em listas, conhecidos como Listas de Certificados Revogados (LCR) ou, em inglês, *Certificate Revocation List* (CRL) [15]. Nesse esquema, a AC produz, assina e divulga, periodicamente, uma lista de certificados revogados. Essa lista geralmente é publicada em servidores de informação de revogação não confiáveis, uma vez que a integridade e autenticidade da lista são garantidas pela assinatura da AC sobre o seu conteúdo. O endereço do diretório onde a lista é disponibilizada é normalmente colocado no próprio certificado. A lista contém, entre outras informações, o número de série dos certificados revogados, a data da publicação da lista e a data da próxima atualização.

Para determinar o estado do certificado, o verificador primeiro obtém a LCR do servidor de informação de revogação indicado no certificado. Em seguida, procura pelo número de série do certificado na lista. Se o número é encontrado, o certificado foi revogado. Em caso negativo, o certificado é considerado como não revogado.

Uma característica inerente a esse método é que o verificador deve obter a LCR de toda uma determinada AC, mesmo que precise da informação de revogação de apenas um certificado. Em ambientes onde o número de certificados revogados é grande, a transmissão de LCRs pode consumir boa parte dos recursos de rede.

Outra característica das LCRs é a **janela de vulnerabilidade**, que consiste no tempo entre a emissão de duas listas sucessivas. Para entender o termo, considere um certificado emitido por uma AC cuja periodicidade de publicação das respectivas LCRs seja Δt. Considere ainda que no instante t, uma lista tenha sido publicada e que num instante imediatamente posterior a t, o usuário percebe que perdeu sua chave privada e comunica o fato à AC, solicitando que ela revogue seu certificado. A informação de que esse certificado foi revogado só será tornada pública com a publicação da próxima lista, emitida no instante $t + \Delta t$. Ou seja, existe um intervalo de vulnerabilidade entre os instantes t e $t + \Delta t$, no qual a AC, mesmo tendo sido informada do comprometimento da chave privada, não é capaz de revogar o certificado.

Uma forma de amenizar o problema da janela de vulnerabilidade é reduzir o tempo entre publicações sucessivas das LCRs, diminuindo o valor de Δt. No entanto, reduzir Δt significa aumentar o número de transmissões e consequentemente os recursos de rede utilizados. Logo, deve haver um equilíbrio entre a janela de vulnerabilidade e a utilização da rede.

Outro problema das LCRs é a concentração de requisições. Para reduzir a janela de vulnerabilidade, os verificadores tentam obter a lista tão logo ela seja publicada, ou seja, no momento da publicação da próxima lista, indicado na lista atual pelo campo *next update* [15]. Isso implica que os verificadores tendem a requerer as LCRs ao mesmo tempo, ocasionando um pico de requisições e de tráfego na rede. Maiores detalhes assim como um estudo quantitativo desse problema podem ser encontrados em [9].

Para reduzir os problemas descritos acima, várias extensões foram propostas para as LCRs. Uma vez que existem na literatura vários trabalhos que fazem uma descrição detalhada de tais extensões, não será refeito tal esforço. Arnes [9] apresenta uma excelente análise das LCRs e suas variações. Abaixo apresenta-se apenas um resumo das principais:

- **Ponto de distribuição de LCRs** (*distribution point CRLs*) [15]: é uma extensão que permite à AC segmentar a sua LCR em diversas partes (os segmentos) e associá-las a um ponto de distribuição.Um ponto de distribuição pode estar em diferentes diretórios em uma mesma máquina ou em diferentes máquinas. Cada certificado contém o endereço do seu ponto de distribuição, permitindo que o verificador obtenha facilmente o segmento contendo a informação de revogação sobre o certificado em questão. A principal vantagem dessa extensão é que o verificador não precisa mais obter toda a LCR para validar um certificado, mas apenas o segmento correspondente. Isso reduz a transferência de dados entre o servidor de informação de revogação e o verificador. Outra vantagem dessa extensão é permitir a distribui-

ção do tráfego entre diferentes pontos, melhorando a escalabilidade das LCRs. A principal desvantagem é que ao validar certificados pertencentes a diferentes segmentos, o verificador pode terminar tendo que obter todos os segmentos, ou seja, não há redução na quantidade de dados a serem transferidos. Pelo contrário, há aumento devido ao custo adicional para estabelecer várias conexões (uma para cada segmento);

- **LCRs Delta** (*Delta CRLs*) [15]: essa extensão tenta reduzir o tamanho das LCRs publicando apenas uma lista (LCR Delta ou LCR incremental) tendo apenas as mudanças em relação à última lista completa divulgada (LCR base). A principal vantagem desse esquema é que ele reduz o tráfego médio entre o verificador e o diretório;

- ***ARLs*** [15]: essa extensão consiste em criar duas listas de revogação: uma para os certificados emitidos para outras ACs, **lista de revogação de autoridades certificadoras** (*Authority Revocation List*) ou ARL, e uma para os certificados emitidos para usuários finais, LCR. Como dificilmente certificados pertencentes às ACs são revogados, as ARLs tendem a ser pequenas ou até mesmos vazias. Essa abordagem é interessante quando a validação do certificado envolve um caminho de certificação, pois, para os certificados das ACs que compõem o caminho, apenas as ARLs precisam ser obtidas. Logo, há redução no tráfego entre o servidor de informação de revogação e o verificador, quando comparado ao esquema que utiliza uma lista única para ACs e usuários finais;

- **LCRs sobrepostas** (*Over-issued CRLs*) [10]: esse esquema permite que múltiplas LCRs possam se sobrepor, ou seja, num mesmo instante de tempo, existem várias LCRs válidas. A vantagem desse esquema é que permite distribuir as requisições das LCRs no tempo, reduzindo o problema da concentração de requisições descrito acima. No entanto, ele tem uma desvantagem séria, pois podem existir duas LCRs válidas com informações conflitantes. Uma consequência direta desse fato é que a propriedade de não repúdio não pode ser mais garantida.

Embora tais extensões amenizem os problemas citados acima, experiências práticas têm mostrado que as LCRs não apresentam boa escalabilidade. Um desses exemplos é apresentado por Nielsen em [29], onde descreve sua experiência no Departamento de Defesa dos Estados Unidos.

4.1.2 *Online Certificate Status Protocol* - OCSP

Nesta proposta, ao invés de uma lista, o verificador obtém apenas a informação sobre o certificado requisitado. Um dos mecanismos mais conhecidos para divulgação de informação de revogação é o OCSP[27]. De forma simplificada, consiste num protocolo para a troca de mensagens contendo tais informações. Existe um servidor de informação de revogação, conhecido como OCSP de consulta[1], que, após ser abastecido com as informações de revogação dos certificados pela própria AC emissora destes (ou por outra entidade

[1]Na falta de uma tradução melhor para *OCSP Responder*.

autorizada por ela), as divulga mediante solicitação do cliente que está verificando o certificado. Para cada solicitação, o OCSP de consulta deve compor uma resposta, contendo o número de série, o estado e outros dados relativos ao certificado, e assiná-la digitalmente.

Para garantir a autenticidade da informação de revogação, o verificador deve conferir a assinatura contida na mesma. Como já foi dito antes, verificar assinaturas digitais é um processo computacionalmente custoso. Observe que num caminho de certificação, a informação de revogação de cada certificado requer uma verificação de assinatura.

A principal vantagem do OCSP é reduzir o tráfego entre o verificador e servidor de informação de revogação (OCSP de consulta), pois apenas a informação de revogação referente ao certificado em questão é transmitida.

Por outro lado, o OCSP de consulta precisa gerar uma assinatura digital para cada solicitação atendida, o que é um processo custoso. Isso tem um impacto significativo na capacidade do OCSP de consulta de processar requisições dos verificadores, reduzindo sua escalabilidade.

4.1.3 Mecanismos baseados em cadeias de resumos

No sentido de reduzir os custos de se validar um certificado, Micali introduziu o *Certificate Revocation System* (CRS) [24, 25], revisado e renomeado para NOVOMODO [26]. Antes de descrever o NOVOMODO, será feita uma breve explanação sobre cadeias de resumos, que são a base de funcionamento do NOVOMODO. A descrição feita a seguir para o NOVOMODO também é valida para o CRS, a não ser por pequenas diferenças que não são significativas para este trabalho.

Cadeias de resumos

Uma cadeia de resumos é uma coleção de valores X_i, $0 \leq i \leq n$, tal que $X_{i+1} = \mathrm{H}(X_i)$ e X_0 é uma sequência de bits aleatória. Constrói-se a cadeia a partir de X_0, também conhecido como raiz ou semente da cadeia, aplicando-se sucessivamente a função resumo $\mathrm{H}()$, como mostrado na Figura 4.1, para obter os demais valores da cadeia. Escreve-se $X_i = \mathrm{H}^i(X_0)$.

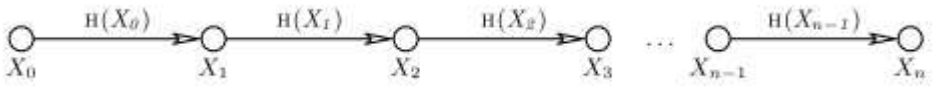


Figura 4.1: Cadeia de resumo

Uma das principais características das cadeias de resumos é a facilidade de determinar se um dado valor X_j pertence ou não à cadeia, dado que se conhece um valor autêntico X_i da mesma, tal que $i > j$. Por exemplo, conhecendo-se o valor de X_n, para determinar se X_j pertence à cadeia, o verificador deve calcular $\mathrm{H}^{n-j}(X_j)$, ou seja, computar a função $\mathrm{H}()$ $(n-j)$ vezes. Se $\mathrm{H}^{n-j}(X_j) = X_n$, então X_j é o $(j+1)$-ésimo elemento da cadeia de resumos $X_0, X_1, \ldots, X_n$. Outra característica importante das cadeias de resumo é que o conhecimento de X_i não dá ao adversário qualquer vantagem para determinar os valores X_j, tal que $j < i$.

Um conceito muito utilizado em cadeias de resumos é o de **transposição**, no qual os valores da cadeia são utilizados (tornados públicos) sucessivamente, em ordem inversa. Ou seja, utilizam-se X_n, X_{n-1}, ..., X_1 e X_0. Para tal é possível usar várias abordagens, com diferentes custos de armazenamento e de processamento. Uma abordagem simples seria armazenar todos os resumos da cadeia em memória e recuperá-los de acordo com a necessidade. Nesse caso, o custo de armazenamento é igual $n.|res|$, em que $|res|$ é o tamanho do resumo, e o custo de processamento é nulo. Outra abordagem simples seria armazenar a raiz da cadeia, X_0, resultando no custo de armazenamento igual a $|res|$ e o custo de processamento igual $n.\mathtt{T}_{res}$, em que $\mathtt{T}_{res}$ é o custo de realizar uma operação de resumo. Resultados obtidos por Jakobsson [16, 11] permitem, armazenando $\log_2 n$ resumos, computar X_j com, no máximo, $\log_2 n$ operações de resumo.

NOVOMODO

Antes de mostrar o funcionamento do NOVOMODO, é preciso deixar claro que ele é baseado em intervalos de tempo, no qual o certificado pode ser válido ou não. Esse intervalo, por exemplo, pode ser um segundo, uma hora, um dia, etc. Por simplicidade, como fez Micali, será utilizado um intervalo de um dia. Isso significa que durante um determinado dia o estado do certificado é único, ou seja, uma vez que ele for determinado, não pode mais ser mudado no mesmo dia. Por exemplo, se no início do dia em questão, o certificado for declarado válido pela AC, ele será aceito como válido até o início do próximo dia, mesmo que no decorrer do dia a AC responsável constate que o certificado deva ser revogado. Em outras palavras, o NOVOMODO apresenta uma janela de vulnerabilidade igual a um dia.

No NOVOMODO, a AC, para cada certificado, escolhe aleatoriamente dois números de $|res|$ bytes (20 bytes considerando a utilização do SHA-1), X_0 e Y_0. Em seguida, gera duas cadeias de resumos: Y_0, Y_1 e $X_0, X_1, \ldots, X_n$. Y_1 e X_n são inseridos no certificado. O valor Y_0 e a sequência de valores X_i, $0 \leq i < n$, são mantidos secretos pela AC. O inteiro n indica o número de intervalos de tempo que compõem o prazo de validade do certificado.

Para determinar o estado do certificado no intervalo j, $j > 0$, a AC divulga ou Y_0 para indicar que o certificado foi revogado ou X_{n-j} para indicar que o certificado não foi revogado. Logo, a cadeia Y_0, Y_1 está relacionada ao estado revogado do certificado enquanto a cadeia $X_0, X_1, \ldots, X_n$ está relacionada ao estado não-revogado. Por exemplo, para um certificado com validade de 365 dias e intervalo de 1 dia ($n = 365$), se o certificado não for revogado, a AC divulga X_{364} no primeiro dia, X_{363} no segundo e assim sucessivamente. Em qualquer dia, se o certificado for revogado, a AC divulga apenas Y_0.

O verificador pode determinar se o certificado foi ou não revogado, verificando se o valor recebido pertence a cadeia Y_0, Y_1 ou a cadeia $X_0, X_1, \ldots, X_n$. Em outras palavras, suponha que o verificador tenha recebido Y_0. Ele computa $\mathtt{H}(Y_0)$ e o compara com Y_1 do certificado sendo validado. Se os valores forem iguais, o verificador conclui que o certificado foi revogado. Por outro lado, se o certificado não tiver sido revogado, o verificador recebe o valor X_{n-j}. Então computa $X'_n = \mathtt{H}^j(X_{n-j})$ e o compara com X_n do certificado. Se os valores forem iguais, o certificado não foi revogado. Se o verificador não puder determinar

à qual cadeia o resumo recebido pertence, então o resumo é considerado inválido.

Observe que a segurança do esquema é dada pelo fato da função de resumo (H()) ser de mão única (*one-way*) e resistente a colisões. Para um intruso forjar o estado do certificado (seja revogado ou não revogado) ele precisa computar o inverso da função de resumo criptográfico ou encontrar uma colisão. Para forjar que um certificado tenha sido revogado, ele precisa obter Y_0. Como um ataque de força bruta está descartado, o intruso precisa computar $Y_0 = \mathrm{H}^{-1}(Y_1)$ ou obter $Y_0' \neq Y_0$, tal que $\mathrm{H}(Y_0') = Y_1$. No caso de forjar um atestado de não revogação do certificado, o intruso, para o intervalo j, deve obter X_{n-j} a partir de X_{n-j+1}, último valor tornado público. Novamente, isso significa computar $X_{n-j} = \mathrm{H}^{-1}(X_{n-j+1})$ ou encontrar $X'_{n-j} \neq X_{n-j}$, tal que $\mathrm{H}(X'_{n-j}) = X_{n-j+1}$. Pelas propriedades da função de resumo criptográfico discutidas anteriormente, tais opções são computacionalmente inviáveis.

Fast Digital Identity Revocation

Aiello et al [8] propuseram um esquema baseado no CRS [25], denominado *Hierarquical Certificate Revocation System* (HCRS), cujo principal objetivo é reduzir a comunicação entre a AC e o servidor de informação de revogação.

O HCRS utiliza cadeias de resumo de forma semelhante ao NOVOMODO para definir o estado do certificado. A diferença entre eles é que, no HCRS, um mesmo resumo pode ser utilizado para determinar o estado de vários certificados. Dessa forma, a AC pode publicar apenas um resumo para vários certificados. Aiello et al mostraram que o número de resumos a ser divulgado é, no máximo, $r.\log_2(v/r)$, em que r é o número de certificados revogados e v o número de certificados emitidos pela AC. Esse valor é menor que os v resumos necessários no NOVOMODO (um para cada certificado emitido pela AC).

Para garantir que apenas um resumo sirva para vários certificados, o certificado deve poder ser validado por diferentes cadeias de resumo, ou seja, um mesmo certificado deve conter vários X_ns. Isso significa um incremento no tamanho do certificado. Aiello mostra que o número de X_ns necessários em cada certificado é igual a $\log_2 v$, onde v é o número de certificados emitidos pela AC.

Embora esse esquema reduza os custos de transmissão entre a AC e o Repositório, ele não traz melhorias para o verificador. Pelo contrário, os custos do verificador aumentam. Como os certificados devem conter mais rótulos, há um aumento do tamanho do certificado, o que tem impacto nos recursos de transmissão utilizados pelo verificador. Por exemplo, para um ambiente com 2^{20} usuários, o certificado deve conter 20 rótulos. Como cada rótulo tem 20 bytes (se for utilizado o SHA-1), o tamanho do certificado sofre um aumento de 400 bytes. Para alguns certificados, isso pode ser o dobro do tamanho original. O número de operações de resumo para verificar o estado do certificado é igual ao do NOVOMODO.

4.1.4 Mecanismos baseados em árvores

Outra abordagem utilizada na revogação de certificados é a baseada em árvores de Merkle, descritas a seguir. Os mecanismos que utilizam árvores de Merkle para gerenciar informa-

ções de revogação são a **árvore de revogação de certificados** (em inglês, *Certification Revocation Tree* - CRT) [17] e a 2-3CRT [28], uma variação da primeira.

Árvores de Merkle

Árvores de Merkle [23], também conhecidas como árvores de resumo, são árvores tais que, a partir do conhecimento do valor da raiz e do valor de alguns dos nós intermediários da árvore, é possível determinar a autenticidade do valor de cada um dos nós folhas realizando um número pequeno de operações de resumo.

As árvores de Merkle são construídas atribuindo-se os valores dos nós folhas e calculando os valores dos nós internos (não folhas) como sendo o resumo do valor dos seus nós filhos. A Figura 4.2 é um exemplo de árvore de Merkle. Para facilitar a identificação dos nós, cada nó foi rotulado com o rótulo do seu pai concatenado com 0 ou 1, dependendo se ele está à esquerda (acima) ou à direita (abaixo), respectivamente, do nó pai. O nó raiz recebeu o rótulo "1".

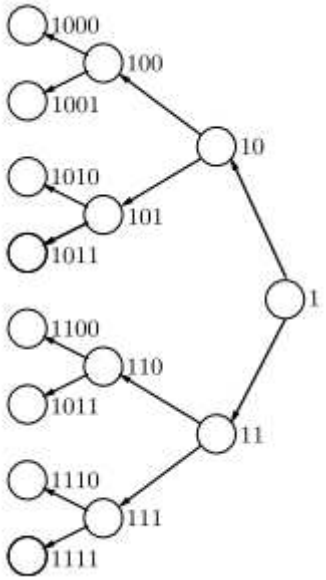


Figura 4.2: Árvore de Merkle

O **caminho de autenticação** de um nó x são os nós que devem ser percorridos, a partir da raiz, para se chegar até o nó x, incluso os nós raiz e x. Na Figura 4.2, para a folha 1001, o caminho de autenticação são os nós rotulados 1, 10, 100 e 1001. O **complemento do caminho de autenticação** de um nó x são todos os nós irmãos dos nós que pertencem ao caminho de autenticação. Na Figura 4.2, o complemento do caminho de autenticação para o nó 1001 são os nós rotulados 11, 101 e 1000.

Para determinar se um nó folha pertence à árvore basta obter o complemento do seu caminho de autenticação e o valor autêntico da raiz da árvore, reconstruir o valor da raiz a partir do complemento e compará-lo com valor autêntico da raiz. Se forem iguais, o nó pertence à árvore. Por exemplo, para que o nó 1001 seja reconhecido como pertencente à árvore da Figura 4.2, devem-se efetuar as seguintes operações ($\text{V}(x)$ indica o valor do nó x):

- $\text{V}(100) = \text{H}(\text{V}(\textit{1000}) \| \text{V}(\textit{1001}))$;
- $\text{V}(10) = \text{H}(\text{V}(\textit{100}) \| \text{V}(\textit{101}))$;
- $\text{V}(1) = \text{H}(\text{V}(\textit{10}) \| \text{V}(\textit{11}))$.

Se $\text{V}(1)$ for igual ao valor autêntico da raiz, então o nó 1001 pertence à árvore de Merkle. Ou, em outras palavras, o valor (conteúdo) do nó em questão foi autenticado.

CRT

Na CRT, os nós folhas da árvore de Merkle são gerados a partir das informações de revogação. Essas informações consistem em intervalos em que o limite inferior é o número de série do certificado revogado e o limite superior indica que os certificados entre o limite inferior e o limite superior não foram revogados. Por exemplo, o intervalo (5,12) indica que o certificado cujo número de série é 5 foi revogado e que os certificados com número de série entre 5 e 12 (6, 7, 8, 9, 10, 11) não foram. Para uma AC cujos certificados de número de série 5, 12, 15, 90, 150, 408 e 409 foram revogados, devem ser definidos os seguintes intervalos: $(\infty, 5)$, $(5, 12)$, $(12, 15)$, $(15, 90)$, $(90, 150)$, $(408, 409)$ e $(409, \infty)$, como na Figura 4.3.

Cada certificado revogado corresponde a um intervalo. Logo, junto à definição do intervalo, podem-se colocar metadados, como data da revogação, motivo, etc. que se referem ao certificado associado ao intervalo. Tal estrutura pode ser utilizada, então, como entrada para uma função de resumo, cujo resultado é o nó folha da árvore (Ver Figura 4.3).

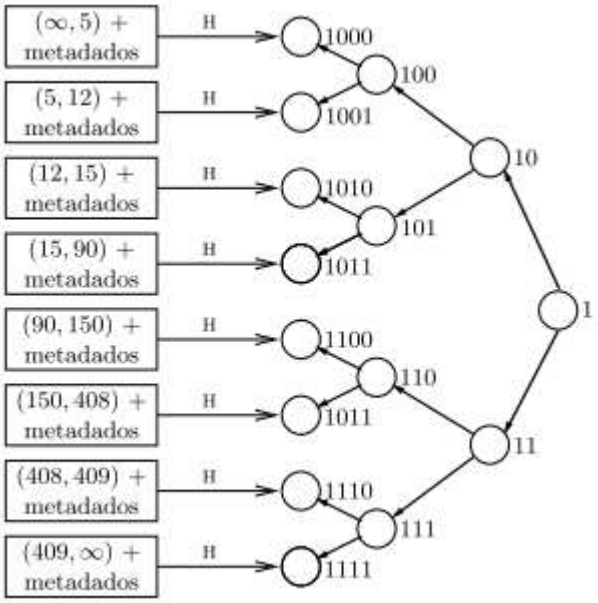


Figura 4.3: CRT

Uma vez que os nós folhas tenham sido definidos, os nós intermediários são gerados como descrito anteriormente até que árvore de Merkle esteja completa. O valor da raiz da árvore, possivelmente acompanhado de metadados, é assinado digitalmente pela AC e

tornado público, através do servidor de informação de revogação. Tal servidor também deve receber a árvore ou dados que lhe permitam reconstrui-la, de modo que ele possa atender as requisições dos clientes (verificador).

Mediante a solicitação da informação de revogação sobre um certificado, o servidor de informação de revogação envia para o verificador: o nó folha cujo intervalo contém o número de série do certificado em questão; o complemento do caminho de autenticação desse nó; e a raiz da árvore assinada digitalmente. O verificador, para aceitar a informação de revogação, deve: verificar a assinatura digital sobre a raiz da árvore para autenticá-la; conferir os metadados que possivelmente acompanham a valor do nó raiz; e computar, a partir do complemento do caminho de autenticação recebido, o valor da raiz e compará-lo com o autêntico. Se ambos forem iguais, a folha associada à informação de revogação é autêntica.

Para o exemplo acima, se o verificador solicita informação de revogação referente ao certificado cujo número de série é 5, ele recebe como resposta a folha contendo o intervalo $(5, 12)$. Como 5 é o início do intervalo, o verificador, após autenticar a folha como descrito anteriormente, conclui que o certificado foi revogado. Por outro lado, se ele solicita informação de revogação sobre o certificado cujo número de série é 10, ele também recebe a folha com o intervalo $(5, 12)$. No entanto, como o valor está contido no intervalo, ele conclui que o certificado não foi revogado (supondo a folha autêntica).

2-3CRT

A CRT como descrito anteriormente, apresenta uma desvantagem. Toda vez que um novo certificado é revogado, a árvore deve ser refeita. Para amenizar tal problema, Naor et Nissim [28] propuseram uma variação desse esquema, utilizando uma árvore conhecida como árvore 2-3, cuja principal propriedade é o fato da atualização só envolver os nós no caminho de autenticação.

Além disso, cada nó folha mantém o número de série do certificado, e não um intervalo. A vantagem dessa modificação é que apenas um número de série (e não um intervalo, definido por dois números de séries) precisa ser enviado. Por outro lado, se o certificado não foi revogado, o SIR precisa enviar dois nós folhas consecutivos da árvore (e os respectivos complementos dos caminhos de autenticação) para provar que o certificado não foi revogado.

Nos demais aspectos, a 2-3CRT se comporta como a CRT.

4.2 Mecanismo integrados

Esta classe aborda a questão de validação como um todo envolvendo tanto o conteúdo do certificado como o estado. ICPA [20], EFFECT [14] e certificados efêmeros (*short lived certificates*) [31] estão entre os principais representantes dessa classe. Também se optou por colocar nessa classe o protocolo SVCP, já que ele permite a transferência completa do processo de validação.

4.2.1 *Standard Certificate Validation Protocol* - SCVP

O SCVP [13] é um protocolo que permite delegar a construção e a validação do caminho de certificação a uma terceira entidade. Esses processos são conhecidos na literatura por **delegação da descoberta do caminho** (em inglês *delegated path discovery* - DPD) e **delegação da validação do caminho** (em inglês *delegated path validation* - DPV).

Uma das principais vantagens do DPD é que permite simplificar a implementação do software cliente, já que este não precisa executar protocolos como HTTP, FTP, LDAP utilizados pelos repositórios de certificados. O cliente também não precisa construir o caminho de certificação entre a sua AC de confiança e o usuário do qual se quer obter a chave pública. Observe que o servidor DPD não precisa ser confiável.

No caso de DPV, o uso do servidor possibilita uma simplificação adicional do software cliente e uma economia adicional e substancial de processamento e banda de transmissão do cliente. Entretanto, claramente, o servidor DPV precisa ser confiável e estar disponível *online*.

Tais características o tornam vulnerável a ataques, por mais bem configurado que seja. O comprometimento do servidor DPV é desastroso, pois todos os clientes que dependem dele para validar certificados ficam à mercê do intruso.

Quando se considera a ICP como um todo, o protocolo SCVP não oferece redução do custo de validação dos certificados, mas apenas uma transferência do cliente para os servidores DPV e DPD.

Vale lembrar que esse protocolo ainda está em discussão pela IETF, especificamente pelo PKIX *Working Group*. Maiores informações podem ser encontradas em [30, 13].

4.2.2 Certificados aninhados

Levi et al [20] propuseram um esquema, denominado **infraestrutura de chaves públicas baseada em certificados aninhados** ou simplesmente ICPA (Adaptação do inglês *Nested Public Key Infrastructure* - NPKI), cujo objetivo é reduzir o custo total da validação de certificados digitais. Esse esquema é baseado em **certificados aninhados** (cn), que são certificados cujo titular é outro certificado, o certificado alvo (ca). Os primeiros garantem que a assinatura sobre o conteúdo dos últimos é válida. O certificado alvo pode ser um certificado tradicional ou outro certificado aninhado.

Conteúdo dos certificados aninhados

O certificado aninhado, assim como o tradicional, é composto pelo seu conteúdo e a assinatura sobre o resumo do seu conteúdo, ou seja, $cn_{ca} = Cont_{cn} \| Sig_{cn}$ (Figura 4.4). O conteúdo do certificado aninhado está relacionado aos requerimentos impostos a ele, que são garantir que o conteúdo do certificado alvo ($Cont_{ca}$) não foi modificado e foi assinado pela AC emissora do certificado. Para satisfazer o primeiro requerimento, o certificado aninhado contém o resumo do conteúdo do certificado alvo ($\text{H}(Cont_{ca})$). Para satisfazer o segundo requerimento, além do resumo, o certificado aninhado também contém a assinatura sobre o conteúdo do certificado alvo, Sig_{ca}. Formalmente, para um certificado

alvo $ca = Cont_{ca} \| Sig_{ca}$, tem-se que $Cont_{cn} = Other \| Sig_{ca} \| \mathrm{H}(Cont_{ca})$. *Other* contém informações secundárias, como identificação de algoritmos.

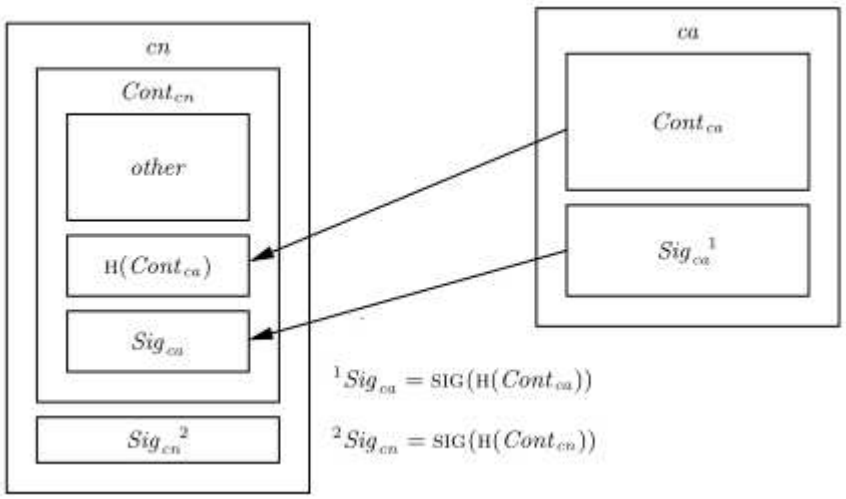


Figura 4.4: Certificado aninhado

Deve-se observar que um certificado aninhado não garante a veracidade do conteúdo do certificado alvo para o qual ele foi emitido. Ele apenas atesta que a assinatura contida no certificado alvo é válida. Para que o cliente (verificador) possa aceitar as informações contidas no certificado alvo como válidas, ele deve confiar na AC que o emitiu.

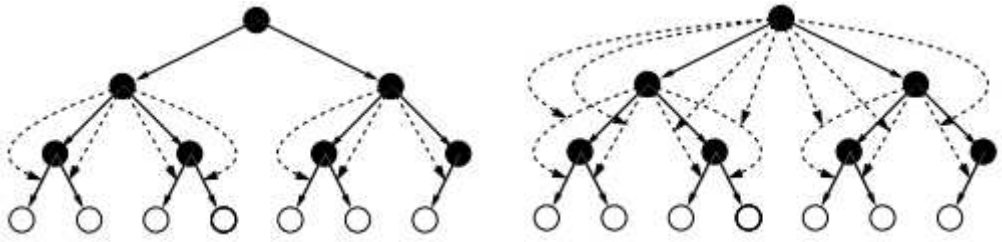
ICPA

Levi et al. propõem dois modelos para a criação de uma ICPA. O primeiro, denominado **modelo de certificação livre**, permite que cada AC escolha o tipo de certificado que ela vai emitir. Nesse caso, o caminho de certificação pode conter tanto certificados aninhados quanto certificados tradicionais, em qualquer sequência, desde que o último seja tradicional. Esse caminho é denominado **caminho de certificação misto**.

O segundo modelo, denominado **transição a partir de uma ICP existente**, consiste em estabelecer uma política para a emissão de certificados aninhados: cada AC deve emitir um certificado aninhado para cada certificado (aninhado ou tradicional) emitido por suas ACs filhas, exceto os emitidos para outra AC[2]. Esse processo, conhecido como **propagação de certificados aninhados**, é mostrado na Figura 4.5, para o caso particular de uma ICP em forma de árvore. Observe que a propagação deve ser feita a partir dos usuários finais (nós folhas) em direção à raiz da hierarquia, seguindo a regra acima. Neste trabalho, a não ser que seja mencionado explicitamente o contrário, o modelo utilizado para construir a ICPA será o de transição a partir de uma ICP existente.

Na Figura 4.6 é mostrado o processo de adição de um novo usuário u à ICPA. Inicialmente deve-se emitir o certificado tradicional para o usuário c. Em seguida, a AC avó do cliente deve emitir o certificado aninhado cn_2. Finalmente, a AC pai da AC avó deve emitir o certificado cn_3 para cn_2.

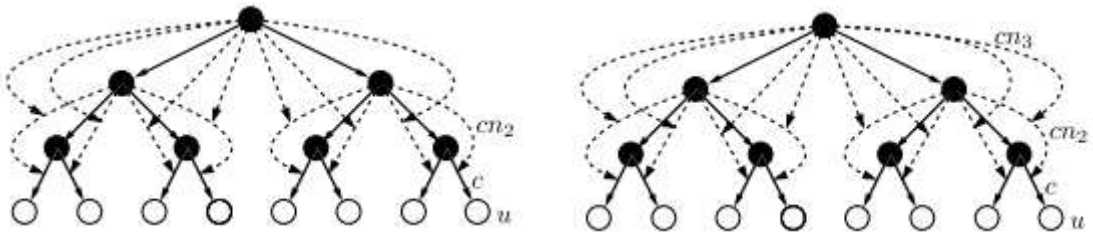
[2]Nesse trabalho considerar-se que tanto os certificados aninhados como os tradicionais são emitidos pela mesma entidade. Por simplicidade, será utilizado o termo AC para designar essa entidade.



(a) (b)

Figura 4.5: Propagação de certificados aninhados numa ICPA

Deve ser destacado que para cada caminho de certificação tradicional existente na ICP original, utilizando-se o método de propagação descrito, é criado um caminho de certificação alternativo na ICPA, composto por certificados aninhados, exceto o último que é um certificado tradicional. Tal caminho é denominado **caminho de certificação aninhado**.



(a) (b)

Figura 4.6: Inserção de um novo usuário na ICP

Verificação

Levi et al distinguem dois métodos para verificação de certificados numa ICPA. O primeiro, denominado **método criptográfico de verificação de certificados aninhados** (do inglês *cryptographyc nested certificates validation method*), consiste em verificar a assinatura contida no certificado aninhado. Dado um determinado certificado aninhado $cn_{ca} = Cont_{cn} \| \text{SIGN}_{d_A}(\text{H}(Cont_{cn}))$ emitido pela AC A, o método consiste dos seguintes passos (supondo o método de verificação de assinaturas baseados no RSA [32]):

- computar $hash \leftarrow \text{VER}_{e_A}(\text{SIGN}_{d_A}(\text{H}(Cont_{cn})))$;
- calcular $hash' \leftarrow \text{H}(Cont_{cn})$;
- comparar $hash'$ com $hash$. Se eles forem iguais, o certificado é autêntico; caso contrário, não.

O segundo método, o **método de verificação de certificados alvos** (do inglês *subject certificate validation method*), consiste em verificar um certificado alvo ca a partir de um certificado aninhado cn_{ca} legítimo emitido para ca. Dado $cn_{ca} = Cont_{cn} \| Sig_{cn}$, tal que $Cont_{cn} = other | hash_{ca} \| Sig_{ca}$ e $hash_{ca} = \text{H}(Cont_{ca})$, a verificação de $ca = Cont_{ca} \| Sig'_{ca}$ consiste em:

- computar $hash \leftarrow \mathrm{H}(Cont_{ca})$;
- comparar $hash$ com $hash_{ca}$ e Sig_{ca} com Sig'_{ca}. Se em ambas as comparações os valores forem iguais, ca é autêntico. Caso contrário não.

Considere um caminho de certificação aninhado $cn_k, cn_{k-1}, \ldots, cn_2, c$, cujo certificado cn_i tenha sido emitido pela AC A_i para o certificado cn_{i-1}, para $2 \leq i \leq k$, mostrado na Figura 4.7. Para verificar tal caminho, o verificador deve possuir todos os certificados desse caminho e a chave pública e_{A_k} de A_k. O primeiro certificado é verificado utilizando-se o método criptográfico de verificação de certificados aninhados e os demais utilizando-se o método de verificação de certificados alvos [20].

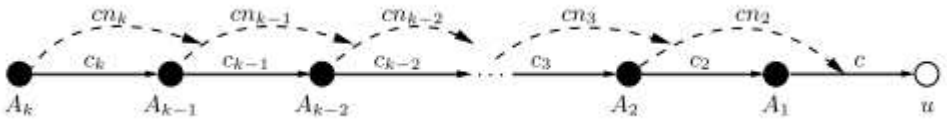


Figura 4.7: Caminho de certificação aninhado

Isso significa dizer que o verificador deve executar uma operação de verificação de assinatura e $k-1$ operações de resumo. Considerando que realizar uma operação de resumo é muito mais eficiente do que realizar uma operação de verificação de assinatura digital, conclui-se que esse esquema permite a verificação de um caminho de certificação tradicional de forma muito mais eficiente (através do caminho de certificação aninhado correspondente).

Revogação

O processo de revogação dos certificados numa ICPA é bem característico e possui três regras importantes, que são:

1. Certificados tradicionais dos usuários finais devem ser revogados utilizando-se mecanismos tradicionais, como OCSP e NOVOMODO.

2. Um certificado tradicional revogado torna o caminho de certificação aninhado associado a ele inútil. O objetivo dos certificados aninhados em um caminho de certificação aninhado é validar o certificado tradicional no final desse caminho. Se o tradicional for revogado, os aninhados não têm mais utilidade e podem ser descartados.

3. Um caminho de certificação aninhado válido não pode começar com um certificado aninhado revogado, mas pode conter certificados aninhados revogados. Considere o caminho de certificação genérico $cn_k, cn_{k-1}, \ldots, cn_2, c$, em que todos os certificados foram emitidos antes do instante t. Considere ainda que no instante t, a AC A_i, $2 \leq i \leq k$, tem sua chave privada comprometida. Logo, é impossível verificar o certificado cn_i, pois qualquer um que possua a chave privada de A_i pode gerá-lo. No entanto, se for considerado o contexto do caminho de certificação aninhado, cn_i ainda pode ser usado, pois o certificado cn_{i+1} emitido antes do comprometimento de A_i (considerando-se que uma AC só emite certificados aninhados para certificados

válidos), torna possível a sua validação. Por outro lado, se um novo certificado foi emitido no instante t_1 ($t_1 > t$), esse certificado não pertencerá a nenhum caminho de certificação que não o tenha como o primeiro; isto porque, uma vez que A_i foi comprometida, nenhuma outra AC irá emitir certificados aninhados para os certificados aninhados emitidos por ela.

As regras acima implicam nos seguintes passos a serem seguidos pelo verificador para verificar um caminho de certificação aninhado:

- determinar o estado (se foi ou não revogado) do primeiro certificado aninhado (regra 3). Para tal, devem-se utilizar mecanismos de revogação de certificados, tais como OCSP e NOVOMODO;
- determinar o estado do último certificado do caminho de certificação, ou seja, do certificado tradicional (regra 1).

Análise

A vantagem da ICPA sobre a ICP tradicional é que ela permite reduzir o custo da validação de um certificado tradicional c, pertencente ao caminho $c_k, c_{k-1}, \ldots, c_1, c$, $k \geq 2$. Numa ICP, esse processo envolve k operações de verificação de assinatura digital e k operações de verificação de informação de revogação. As últimas podem ser operações de verificação de assinatura digital (OCSP) ou operações de resumo (NOVOMODO). Já numa ICPA, o caminho de certificação aninhado, $cn_k, cn_{k-1}, \ldots, cn_1, c$, permite que c seja validado com uma operação de verificação de assinatura, $k-1$ operações de resumo e duas operações de verificação de informação de revogação.

No entanto, esse esquema apresenta algumas desvantagens em relação ao tradicional, que advém do fato de que as ACs superiores estão diretamente envolvidas com a emissão de certificados aninhados para os clientes de suas ACs subordinadas. As desvantagens são a sobrecarga e a maior exposição das ACs e o atraso na propagação dos certificados aninhados.

A sobrecarga das ACs é devida ao mecanismo de propagação de certificados aninhados. Sempre que um certificado é emitido para um usuário final, todas as ACs superiores à AC emissora do certificado do usuário final devem emitir um certificado aninhado. Particularmente, numa ICP em forma de árvore, isso significa que quanto mais próxima da raiz a AC está, maior será o número de certificados que ela deve emitir. Por exemplo, o número de certificados aninhados emitidos pela AC raiz é igual ao número de certificados emitidos para usuários finais na ICPA. Logo, há um aumento significativo no trabalho das ACs.

Esse problema se tornaria ainda maior se se permitisse utilizar esse mecanismo para certificação cruzada. Nesse caso, cada uma das duas ACs envolvidas deveria emitir um número de certificados aninhados igual ao número de clientes subordinados à outra AC. Particularmente no caso de uma certificação cruzada entre duas ACs raízes, o número adicional de certificados aninhados a serem emitidos por uma das ACs é igual ao número de clientes da ICPA à qual ela não pertence.

Outro problema é a maior exposição das ACs. Como foi visto, toda vez que é emitido um certificado para um usuário final, as AC superiores à AC que emitiu o certificado terão que emitir certificados aninhados. Isso implica que constantemente as ACs devem ser acionadas para determinar se há certificados aninhados a serem emitidos. Como consequência, tem-se uma maior exposição das ACs, e consequentemente um risco maior de comprometimento das mesmas.

Finalmente, viu-se que a propagação de certificados aninhados é feita de forma serial. Ou seja, para um caminho de certificação qualquer, a AC superior necessita esperar até que a AC subordinada tenha emitido o certificado aninhado. Logo, o tempo de propagação de certificados aninhados tende a ser longo. O resultado é que enquanto não houver um caminho de certificação aninhado para o certificado tradicional em questão, a validação deve ser feita do modo tradicional, muito mais custoso.

4.2.3 EFFECT

EFFECT (abreviação do inglês *Easy Fast Efficient Certification Techinique*, cuja tradução pode ser técnica de certificação fácil, rápida e eficiente) foi proposto por Gassko et al [14] e sua principal característica é abolir os certificados digitais assinados individualmente e também a necessidade de mecanismos de revogação explícitos como LCR, OCSP e CRT. Em seu lugar é utilizada uma árvore denominada *Certification Verification Tree* (CVT), que permite que a integridade e o estado do certificado sejam verificados simultaneamente.

Essa árvore é construída de forma semelhante à mostrada na Seção 4.1.4. Cada nó folha da árvore é composto pelo conteúdo do certificado e pelo resumo desse conteúdo. Os nós intermediários são obtidos calculando-se o resumo sobre a concatenação do valor dos seus nós filhos, como mostrado na Figura 4.2. Ao valor da raiz obtido, RV na nomenclatura utilizada por Gassko et al, são adicionados outros metadados, como data, hora, etc. Esses dados são assinados digitalmente e tornados públicos.

A validação do certificado é feita da seguinte forma: o verificador obtém o nó folha, contendo o certificado, e o complemento do caminho de autenticação desse nó. De posse desses valores, computa o valor da raiz da árvore, RV'. O verificador também determina que o valor de RV recebido é autentico, através verificação da assinatura digital. Então ele compara RV com RV'. Se os valores forem iguais, o certificado é aceito como válido (ou seja, ele está integro e não foi revogado).

O EFFECT na verdade é muito semelhante ao CRT. A principal diferença é que a árvore construída permite determinar, além do estado do certificado, a sua autenticidade.

4.2.4 Certificados efêmeros

Essa abordagem consiste em reduzir o prazo de validade do certificado de forma que não seja necessário verificar se o certificado foi revogado ou não. Por exemplo, um certificado poderia ser emitido com validade de um dia. Isso significa que ele só seria válido no dia em que foi emitido. Para utilizar a chave no dia seguinte, seria necessário emitir um novo certificado. Uma das primeiras propostas nesse sentido foi feita por Rivest [31].

4.3 Custos de validação

Nesta seção será feita uma análise dos custos de validação dos certificados. Serão analisados os custos dos principais mecanismos descritos acima, no que tange ao custos de processamento (C_C e C_A) e ao custos de transmissão (C_T e C_R) na infraestrutura de chaves públicas.

Tais custos serão analisados dando-se ênfase aos custos do verificador, que pode ser um usuário final ou uma entidade que provê tal serviço para outros, por exemplo, por meio do protocolo SCVP. Também serão considerados os custos do resto da infraestrutura, incluindo autoridades certificadoras e servidores de informação de revogação. Para efeitos de comparação, será utilizada uma situação em o verificador se incube de validar um caminho de certificação com k certificados.

4.3.1 Mecanismos de verificação de informação de revogação

Para os mecanismos de informação de revogação, C_C, C_T, C_R e C_A apresentam duas componentes distintas: uma devida aos certificados (respectivamente $C_C(c)$, $C_T(c)$, $C_R(c)$ e $C_A(c)$) e outra devida às informações de revogação (respectivamente $C_C(ir)$, $C_T(ir)$, $C_R(ir)$ e $C_A(ir)$). Logo, pode-se escrever:

$$C_C = C_C(c) + C_C(ir) \quad (4.1)$$
$$C_T = C_T(c) + C_T(ir) \quad (4.2)$$
$$C_R = C_R(c) + C_R(ir) \quad (4.3)$$
$$C_A = C_A(c) + C_A(ir) \quad (4.4)$$

O valor de $C_R(c)$ para todos os mecanismo desta classe (LCR, OCSP, NOVOMODO e CRT/23CRT) é igual a $k.|sig|$, em que k é o número de certificados no caminho de certificação sendo verificado e $|sig|$ é o tamanho de uma assinatura digital. De fato, o verificador deve obter cada um dos certificados, cada qual contendo uma assinatura digital.

O ASR deve disponibilizar os certificados para o verificador. Para cada certificado requisitado pelos verificadores, o ASR tem custo de transmissão igual a $|sig|$. Supondo-se que em um determinado intervalo de tempo, são feitas q solicitações de certificados, o custo de transmissão $C_T(c) = q.|sig|$ para todos os mecanismos desta classe.

O custo $C_C(c)$, também igual para todos os mecanismos desta classe, é $C_C(c) = k.\mathrm{T}_{ver}$, em que T_{ver} é o custo da operação de verificação de assinatura. Esse custo corresponde a operação de verificação de assinatura, uma por certificado, para determinar a autenticidade dos mesmos.

Considerando-se que as ACs gerenciam, em média, v certificados digitais, com validade de t intervalos de tempo (dias, por exemplo) e que os certificados são emitidos uniformemente no tempo, têm-se, em cada intervalo, v/t certificados sendo emitidos (e outros v/t expirando). Logo, $C_A(c) = \frac{v}{t}\mathrm{T}_{sig}$ para todos os mecanismos desta classe.

Os custos $C_A(ir)$, $C_T(ir)$, $C_R(ir)$ e $C_C(ir)$ variam de acordo com o mecanismo utilizado

e são mostrados abaixo. A Seção 4.3.3 (Tabelas 4.1, 4.2, 4.3 e 4.4) traz um resumo dos custos apresentados e também os custos totais de processamento no ASR (C_A), de processamento no verificador (C_C) e de transmissão do verificador (C_R) e de transmissão do ASR (C_T) para os mecanismos discutidos.

LCR

Para a emissão das LCRs, é necessário que o ASR compute uma assinatura digital para cada lista emitida. O número de listas a serem emitidas depende do intervalo entre a emissão de LCRs sucessivas. Definindo j como a frequência de emissão de LCRs, por exemplo, em emissões por dia, o custo de processamento do ASR para emitir informações de revogação é $C_A(ir) = j.\mathrm{T}_{sig}$.

O custo de processamento do verificador para atestar a autenticidade da lista é o custo de verificar uma assinatura digital .Como o verificador deve obter uma LCR para cada certificado do caminho de certificação, então $C_C(ir) = k.\mathrm{T}_{ver}$.

O custo de transmissão do verificador é igual ao tamanho da LCR. Logo, o custo de transmissão é $C_T(ir) = k(|sig| + r.|sn|)$, em que $|sn|$ é tamanho utilizado para indicar o número de série do certificado e r é o número médio de certificados revogados.

Finalmente, o custo de transmissão do ASR é o mesmo, por requisição, do verificador. Se q for o número de requisições atendidas, então $C_T(ir) = q.(|sig| + r.|sn|)$.

OCSP

Para emitir cada informação de revogação solicitada, o OCSP de consulta (ASR) deve efetuar uma assinatura digital. Logo, o custo de processamento dele é $C_A(ir) = q.\mathrm{T}_{sig}$. Como o custo de transmissão para responder cada requisição é $|sig|$, tem-se que $C_T(ir) = q.|sig|$.

O custo de processamento do verificador é o de conferir uma assinatura digital para cada informação de revogação, o que resulta em $C_C(ir) = k.\mathrm{T}_{ver}$. O custo de transmissão do verificador também é $|sig|$ por requisição. No entanto, ele realiza k requisições, uma por certificado, resultando em $C_R(ir) = k.|sig|$.

NOVOMODO

Inicialmente, considere o custo de transmissão entre o verificador e o ASR. Esse custo é sempre de 20 bytes (ainda considerando o uso do SHA-1), para cada certificado. Logo, $C_R(ir) = k.|res|$ e $C_T(ir) = q.|res|$, em que $|res|$ é o tamanho de um resumo criptográfico. Esse custo é significativamente menor do que os dos demais esquemas vistos, já que o tamanho de uma assinatura digital é muito maior do que o de um resumo. Por exemplo, para o RSA e o SHA-1 os tamanhos são, respectivamente, 1024 e 160 bits.

O custo de processamento do verificador $C_C(ir)$ depende do tamanho da cadeia de resumo, que é igual a n (que também pode ser definido como t/j) . O número de operações de resumo a serem realizadas pelo verificador é um valor entre 1 (no primeiro intervalo) e n (no último intervalo) ou $n/2$ na média. Logo, para um caminho de certificação, $C_C(ir) = k\frac{n}{2}\mathrm{T}_{res}$. Observar-se que se a aplicação possui requisitos de tempestividade

severos, por exemplo, de 1 hora ou 15 segundos (o que já pode ser considerado, para ambientes como a Internet, como sendo de tempo real [26]), o custo pode ser proibitivo. No primeiro caso, $n = 8760$ e no segundo $n = 2.102.400$, ou seja, o número médio de operações é, respectivamente, 4.380 e 1.051.200.

Do ponto de vista do ASR tanto o fator processamento quanto o fator armazenamento devem ser considerados cuidadosamente para valores grandes de n. Até o momento foi suposto que o ASR mantém todos os valores intermediários da sequencia de resumo. No entanto, para o caso de intervalos de 15 segundos ($n = 2.102.400$), o espaço requerido é aproximadamente 40MB por certificado, o que pode ser inviável. Por outro lado, observa-se que o ASR pode manter apenas X_0 e calcular X_{n-j} para cada intervalo. Esse custo, na média, é igual ao custo do verificador, para cada certificado. Dependendo do número de certificados que o ASR deve manusear, pode não ser possível computar todos os valores necessários, principalmente para intervalos pequenos. Logo, existe um equilíbrio a ser mantido entre armazenamento e processamento. Micali sugere armazenar valores intermediários da função de resumo, por exemplo, como os definidos por Jakobsson [16, 11], que permite, armazenando $\log_2 n$ valores, computar X_i com, no máximo, $\log_2 n$ operações de resumo. Lembrando que para os certificados revogados esse cálculo não é necessário (basta o ASR disponibilizar Y_0), tem-se que $C_A(ir) = j(v - r)\log_2 n.\mathrm{T}_{res}$.

CRT

Como foi descrito, para cada CRT divulgada, o ASR computa uma assinatura sobre o valor da raiz , o que, para uma atualização com frequência j, resulta em $j.\mathrm{T}_{sig}$. Além disso para obter a raiz(e por consequência a árvore), para um ASR que possui um número médio de certificados revogados igual a r, são necessárias $2r - 1$ operações de resumo. Logo, o custo para emitir CRTs é $C_A(ir) = j((2r - 1)\mathrm{T}_{res} + \mathrm{T}_{sig})$.

O custo de transmissão do verificador envolve, para cada certificado do caminho, transmitir uma assinatura digital e $\log_2 r$ resumos, ou seja, $C_R(ir) = k.(|sig| + \log_2 r.|res|)$. O custo de transmissão do ASR é $C_T(ir) = q(|sig| + \log_2 r.|res|)$.

Para processar a informação de revogação, o verificador deve conferir a autenticidade do valor da raiz da CRT, através da verificação da assinatura digital, e reconstruir a raiz, o que despende $\log_2 r$ operações de resumo, resultando em $C_C(ir) = k(\mathrm{T}_{ver} + \log_2 r.\mathrm{T}_{res})$.

4.3.2 Mecanismos integrados

Certificados efêmeros

Esse esquema não utiliza informações de revogação. Logo, não existem custos associados à verificação do estado dos certificados. Por consequência: $C_T = q.|sig|$, $C_R = k.|sig|$ e $C_C = k.\mathrm{T}_{sig}$.

Por outro lado, é atribuído um custo maior ao ASR, que deve reemitir o certificado para atender aos requisitos de tempestividade. Assumindo que a frequência com que os certificados sejam reemitidos seja j, tem-se que $C_A = j.v.\mathrm{T}_{sig}$.

EFFECT

No EFFECT, a AC constrói apenas uma árvore que por si só permite a validação do certificado. Para construir tal árvore é necessário executar $2v-1$ operações de resumo e uma operação de assinatura digital. Logo, o custo de construção da árvore é $\mathrm{T}_{sig} + (2v-1)\mathrm{T}_{res}$. Logo, $C_A = j(\mathrm{T}_{sig} + (2v-1)\mathrm{T}_{res})$, em que j é a frequência com que a árvore é atualizada.

Para validar cada certificado, o verificador necessita do valor da raiz assinado e do complemento do caminho de autenticação do nó em questão, que contém $\log_2 v$ nós. Logo, $C_T = q(|sig| + \log_2 v|res|)$ e $C_R = k(|sig| + \log_2 v|res|)$.

Finalmente, o custo de validação do caminho de certificação do verificador é dado por $k(\mathrm{T}_{ver} + \log_2 v.\mathrm{T}_{res})$. Ou seja, o custo de conferir a assinatura sobre o valor da raiz adicionado do custo de reconstruir a raiz a partir do complemento do caminho de autenticação. Observe também que, nesse caso, não há uma componente devida à assinatura sobre os certificados, como há no CRT e 23CRT.

ICPA

A ICPA necessita de uma operação de assinatura digital para validar o primeiro certificado do caminho de validação e $k-1$ operações de resumo para os demais , conforme demonstrado no item Análise da Seção 4.2.2. Além disso, para verificar o estado do primeiro certificado (emitido pela AC âncora) e do certificado do usuário final, é necessário utilizar um mecanismo auxiliar de revogação, por exemplo, o NOVOMODO. Nesse caso, são necessárias em média n $(2.\frac{n}{2})$ operações de resumo. Logo, $C_C = \mathrm{T}_{ver} + (k+n-1)\mathrm{T}_{res}$.

Pelo que foi dito, deduz-se que $C_T = q.(|sig| + |res|)$. Para o verificador, o custo $C_R = k.|sig| + 2.|res|$.

Finalmente, abordam-se os custos de emissão dos certificados pela AC. Nesse aspecto, a ICPA se diferencia dos demais mecanismos pela emissão de certificados aninhados. Assumindo que o número de certificados aninhados seja v_{cn}, o custo de emissão de certificados será $C_A(c) = \frac{v}{t}\mathrm{T}_{sig} + v_{cn}\mathrm{T}_{sig}$. Além disso, tem-se o custo de emissão das informações de revogação $C_A(ir) = (v-r).j.\log_2 n.\mathrm{T}_{res}$, igual ao NOVOMODO. No próximo capítulo, o custo da emissão dos certificados aninhados será abordado com maior profundidade.

4.3.3 Resumo dos custos

A Tabela 4.1 é o resumo dos custos de processamento para gerar/emitir os certificados e as informações de revogação do ASR. O significado das variáveis utilizadas é mostrado na Tabela 4.5. A Tabela 4.2 mostra os custos de processamento do verificador para validar os certificados.

Observando a Tabela 4.2, nota-se que o menor custo para validação do caminho de certificação é o apresentado pela ICPA, utilizando como mecanismo de revogação o NOVOMODO. De fato, ele apresenta, independentemente do tamanho do caminho de certificação (k), custo devido a operações de assinatura digital constante e unitário. Todos os demais mecanismos apresentados possuem tal custo em função de k.

Sob uma observação mais cuidadosa, vê-se que o custo de validar o certificado na ICPA, é composto em parte por operações de resumo, que não foram mencionadas acima.

Mecanismo	**ASR**		
	$C_A(c)$	$C_A(ir)$	C_A
LCR	$\frac{v}{t}.\mathrm{T}_{sig}$	$j.\mathrm{T}_{sig}$	$(\frac{v}{t}+j)\mathrm{T}_{sig}$
OCSP	$\frac{v}{t}.\mathrm{T}_{sig}$	$q.\mathrm{T}_{sig}$	$(\frac{v}{t}+q)\mathrm{T}_{sig}$
NOVOMODO	$\frac{v}{t}.\mathrm{T}_{sig}$	$j(v-r)\log_2 n.\mathrm{T}_{res}$	$\frac{v}{t}.\mathrm{T}_{sig}+j(v-r)\log_2 n.\mathrm{T}_{res}$
CRT/2-3CRT	$\frac{v}{t}.\mathrm{T}_{sig}$	$j((2r-1)\mathrm{T}_{res}+\mathrm{T}_{sig})$	$(\frac{v}{t}+j)\mathrm{T}_{sig}+j(2r-1)\mathrm{T}_{res}$
ICPA	$(\frac{v}{t}+v_{cn}).\mathrm{T}_{sig}$	$j(v-r)\log_2 n.\mathrm{T}_{res}$	$(\frac{v}{t}+v_{cn}).\mathrm{T}_{sig}+$ $j(v-r)\log_2 n.\mathrm{T}_{res}$
EFFECT	-	-	$j(\mathrm{T}_{sig}+(2v-1)\mathrm{T}_{res})$
Efêmeros	-	-	$j.v.\mathrm{T}_{sig}$

Tabela 4.1: Custos de processamento - ASR

Mecanismo	**Verificador**		
	$C_C(c)$	$C_C(ir)$	C_C
LCR	$k.\mathrm{T}_{ver}$	$k.\mathrm{T}_{ver}$	$2k.\mathrm{T}_{ver}$
OCSP	$k.\mathrm{T}_{ver}$	$k.\mathrm{T}_{ver}$	$2k.\mathrm{T}_{ver}$
NOVOMODO	$k.\mathrm{T}_{ver}$	$k.\frac{n}{2}.\mathrm{T}_{res}$	$k.\frac{n}{2}.\mathrm{T}_{res}+k.\mathrm{T}_{ver}$
CRT/23CRT	$k.\mathrm{T}_{ver}$	$k.\log_2 r.\mathrm{T}_{res})$	$k(\mathrm{T}_{ver}+\log_2 r.\mathrm{T}_{res})$
ICPA	-	-	$\mathrm{T}_{ver}+(k+n-1).\mathrm{T}_{res}$
EFFECT	-	-	$k(\mathrm{T}_{ver}+\log_2 v.\mathrm{T}_{res})$
Efêmeros	-	-	$k.\mathrm{T}_{ver}$

Tabela 4.2: Custos de processamento - verificador

No entanto, como as operações de resumo são muito mais rápidas que as operações de verificação de assinatura, esses valores não influenciam significativamente no custo total, exceto para valores muito grandes de n. Por exemplo, para $n = 365$, é necessário efetuar $364 + k$ operações de resumo, cujo custo é menor do que o de k operações de verificação de assinatura digital.

Logo, para validar um caminho de certificação, com vários certificados, as ICPAs seriam o mecanismo mais indicado, pelo ponto de vista do custo de validação do verificador. No entanto, ainda considerando a Tabela 4.1, vê-se que este ganho no verificador é pago com o custo adicional de emissão dos certificados aninhados. Como visto na Seção 4.2.2, esse custo pode tornar a estrutura inviável para ICPs de grande porte com vários níveis de ACs.

A Tabela 4.3 resume o custo de transmissão do verificador nos esquemas analisados. Ela mostra que os certificados efêmeros têm o menor C_R, já que sua utilização não requer informações de revogação. A ICPA é o segundo método a apresentar o menor C_R, seguido pelo NOVOMODO. Considerando que o tamanho de um resumo é pequeno, em torno de 20 bytes, a diferença desse custo entre o certificados efêmeros e a ICPA é desprezível, pois, independente do tamanho do caminho de certificação, a diferença será sempre de 40 bytes. No caso do NOVOMODO, a diferença depende do tamanho do caminho de certificação. No entanto, ela ainda é pequena, pois para $k \leq 10$, que compreende os valores de k para o universo das aplicações reais, a diferença para o caminho de certificação ainda é no máximo igual a 200 bytes.

A Tabela 4.4 mostra os custos de transmissão do ASR. Nesse caso, novamente, os

Mecanismo	**Verificador**		
	$C_R(c)$	$C_R(ir)$	C_R
LCR	$k.\|sig\|$	$k.(\|sig\| + r.\|sn\|)$	$k(2\|sig\| + r.\|sn\|)$
OCSP	$k.\|sig\|$	$k.\|sig\|$	$2.k.\|sig\|$
NOVOMODO	$k.\|sig\|$	$k.\|res\|$	$k(\|sig\| + \|res\|)$
CRT/23CRT	$k.\|sig\|$	$k(\|sig\| + \log_2 r.\|res\|)$	$k(2\|sig\| + \log_2 r.\|res\|)$
ICPA	-	-	$k.\|sig\| + 2\|res\|$
EFFECT	-	-	$k(\|sig\| + \log_2 v.\|res\|)$
Efêmeros	-	-	$k.\|sig\|$

Tabela 4.3: Custo de transmissão - verificador

certificados efêmeros tem o melhor desempenho, seguidos pela ICPA e pelo NOVOMODO. Diferentemente do custo de transmissão do verificador, o custo de transmissão do ASR, na ICPA e no NOVOMODO, depende do número de requisições feitas. A comparação entre os últimos com os certificados efêmeros mostra que os estes requerem $|res|$ bits de dados a menos por certificado. Para encerrar, observe que quando o ASR é responsável por um certificado intermediário, não há necessidade da informação de revogação, e o custo de transmissão na ICPA se iguala ao dos certificados efêmeros.

Mecanismo	**ASR**		
	$C_T(c)$	$C_T(ir)$	C_T
LCR	$q.\|sig\|$	$q.(\|sig\| + r.\|sn\|)$	$q(2\|sig\| + r.\|sn\|)$
OCSP	$q.\|sig\|$	$q.\|sig\|$	$2.q.\|sig\|$
NOVOMODO	$q.\|sig\|$	$q.\|res\|$	$q(\|sig\| + \|res\|)$
CRT/23CRT	$q.\|sig\|$	$q(\|sig\| + \log_2 r.\|res\|)$	$q(2\|sig\| + \log_2 r.\|res\|)$
ICPA	-	-	$q.(\|sig\| + \|res\|)$
EFFECT	-	-	$q(\|sig\| + \log_2 v.\|res\|)$
Efêmeros	-	-	$q.\|sig\|$

Tabela 4.4: Custo de transmissão - ASR

Resumindo, a ICPA apresenta, para o ambiente proposto, o melhor custo de validação do certificado e também os custos de transmissão muito próximos aos dos certificados efêmeros, que é o mecanismo com melhor custo de transmissão. Como foi visto, o única desvantagem da ICPA é o custo adicional de emissão dos certificados aninhados, que a torna inviável para ICPs de grande porte. No próximo capítulo, será abordado esse custo com mais profundidade.

Parâmetro	Significado
k	Número de certificados que compõem o caminho de certificação.
j	Taxa de atualização das informações de revogação. Indica a frequência com que as informações de revogação são divulgadas, medida em ocorrências em um determinado intervalo, por exemplo, hora, dia, semana.
q	Número de requisições feitas ao servidor de informação de revogação, também feitos num determinado intervalo.
v	Número médio de certificados tradicionais gerenciados pela AC.
v_{cn}	Número médio de certificados aninhados gerenciados pela AC.
r	Número médio de certificados revogados por AC, cujo prazo de validade ainda não tenha expirado.
t	Tempo médio de vida do certificado.
T_{sig}	Tempo para computar uma assinatura digital.
T_{ver}	Tempo para verificar uma assinatura digital.
T_{res}	Tempo para efetuar uma operação de resumo.
$\|res\|$	Tamanho do resumo.
$\|sig\|$	Tamanho da assinatura digital.
$\|sn\|$	Tamanho do número de série do certificado.

Tabela 4.5: Parâmetros

Capítulo 5

ICPAm

5.1 ICPAm

Nesta seção é proposto um novo modelo para a geração da ICPA, resultante da modificação do modelo transição a partir de uma ICP existente. Para diferenciá-los, será acrescentando um m minúsculo ao termo ICPA para se referir ao novo modelo.

A modificação proposta consiste em decompor a validação do caminho de certificação em duas etapas: a validação do caminho de certificação até a AC emissora do certificado do usuário final (indicado por I na Figura 5.1) e a validação do certificado do cliente emitido por essa AC (II). De fato, a validação de (I) permite obter a chave pública de A_1. De posse dessa chave, o certificado do usuário (II) pode ser validado.

A primeira etapa, (I), é validada utilizando-se o caminho $cn_k, cn_{k-1}, \ldots, cn_2, c_1$ enquanto a segunda (II) é validada de forma tradicional (verificação da assinatura do certificado mais um método de revogação, por exemplo OCSP ou NOVOMODO). (I) e (II) também podem ser vistos como um único caminho misto, composto por $k-1$ certificados aninhados e 2 certificados tradicionais.

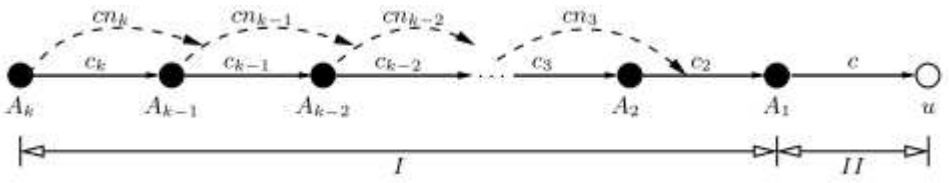
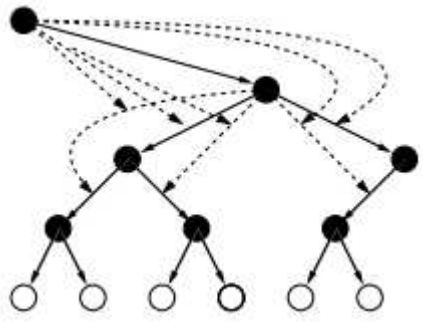


Figura 5.1: Decomposição do caminho de certificação

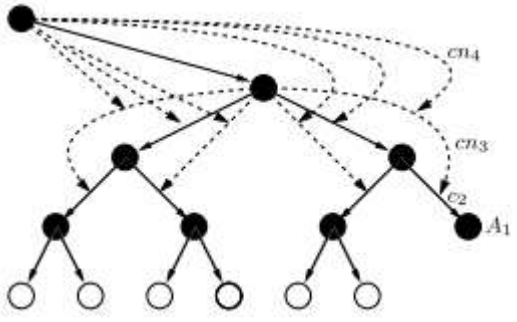
Para que a nova abordagem seja possível é necessário existir um caminho de certificação aninhado entre a AC de confiança do verificador A_k e a AC emissora do certificado do usuário final A_1 (como o mostrado na Figura 5.1). Isso significa que se deve redefinir a regra para emissão de certificados aninhados. A nova regra é a seguinte: uma AC deve emitir certificados aninhados para os certificados, emitidos pelas suas filhas, que são aninhados ou são tradicionais emitidos para outras ACs (suas netas). As ACs não emitem certificados aninhados para os usuários finais.

A Figura 5.2(a) mostra os certificados emitidos segundo essa nova regra. Foi inserido mais um nível de ACs na hierarquia para mostrar que a AC pai deve emitir certificados

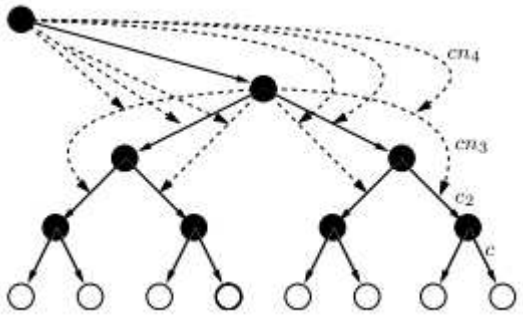
aninhados para os certificados emitidos pela sua filha que: (i) são aninhados ou (ii) são tradicionais emitidos para outra AC.



(a) Propagação de certificados aninhados



(b) Inserção de uma AC



(c) Inserção de usuários finais

Figura 5.2: Modificações introduzidas na ICPAm

Na figura 5.2(b), mostra-se a propagação de certificados quando uma nova AC A_1 é inserida na ICPAm. Essa propagação é semelhante à propagação na ICPA. A diferença é que a propagação é feita a partir do certificado da AC e não do usuário final.

A Figura 5.2(c) mostra que a inserção de usuários finais na ICPAm não implica na emissão de nenhum certificado aninhado.

Análise: A principal mudança em relação à ICPA é que as ACs ascendentes não estão mais diretamente envolvidas com a propagação dos certificados dos usuários finais. Ou, em outras palavras, não existe tal propagação. Só existe a propagação de certificados aninhados para certificados emitidos para ACs.

A consequência dessa mudança é que os problemas da ICPA indicados anteriormente no Capítulo 4 são contornados. Ou seja, a sobrecarga imposta às ACs é reduzida, a exposição das ACs também é reduzida e o tempo de propagação é eliminado para os certificados emitidos para usuários finais.

A sobrecarga das ACs superiores da ICPAm é reduzida, pois elas só precisam propagar certificados aninhados para as suas ACs descendentes, cujo número é normalmente pequeno em relação ao número de clientes. Na Seção 5.2.1 é feita uma avaliação da ICPAm que justifica essa afirmativa.

Também é possível permitir a certificação cruzada entre ICPAms. Observe que agora o custo, no pior caso, quando duas ACs raízes estão estabelecendo certificação cruzada, é

emitir um certificado aninhado para cada AC da ICPAm da outra AC. Como já foi dito, o número de ACs é muito menor que o número de usuários, o que significa que o custo de emissão dos certificados aninhados nesse caso é significativamente menor.

A exposição das ACs é reduzida, pois uma AC superior só precisa emitir certificados aninhados quando uma nova AC subordinada é inserida na ICPAm, uma tarefa rara e que pode ser feita de forma planejada.

O tempo de propagação para os clientes inexiste. Para as ACs, esse tempo pode ser desprezado, pois pode se considerar que para uma AC estar operacional a propagação dos certificados aninhados referentes ao certificado dela deve estar completa.

A desvantagem é que há um aumento no custo de validação do certificado do usuário final. Na próxima seção são mostrados resultados que quantificam esse aumento.

5.2 Análise de custos das ICPAs

O custo de validação do verificador (C_C) na ICPAm, considerando o NOVOMODO como mecanismo de verificação de informação de revogação, é muito similar ao da ICPA. Na ICPAm, como foi visto, o caminho de certificação entre a AC âncora e o usuário final pode ser decomposto em um caminho aninhado de $k-1$ certificados ($k-2$ aninhados e um tradicional) mais um tradicional (ver Figura 5.1). Logo, pode-se escrever:

$$\begin{aligned} C_C &= \mathrm{T}_{ver} + (k-2+\frac{2n}{2}).\mathrm{T}_{res} + \mathrm{T}_{ver} + \frac{n}{2}.\mathrm{T}_{res} \\ &= 2\mathrm{T}_{ver} + (k-2+\frac{3n}{2}).\mathrm{T}_{res} \end{aligned}$$

O custo de transmissão do verificador também é muito semelhante ao do apresentado pela ICPA. No caso da ICPAm, o verificador deve apenas obter uma informação de revogação adicional, o que resulta em $C_R = k.|sig| + 3|res|$.

O custo de transmissão do ASR é igual ao da ICPA, ou seja, $C_T = q.(|sig| + |res|)$.

Finalmente, tem-se o custo de processamento do ASR, C_A. Viu-se no capítulo anterior, para a ICPA, que $C_A = (\frac{v}{t} + v_{cn}).\mathrm{T}_{sig} + j(v-r)\log_2 n.\mathrm{T}_{res}$. Exceto por v_{cn}, o custo da IPCAm é o mesmo. Determinar v_{cn} é difícil, pois tal componente depende do número de certificados aninhados, que por sua vez depende da topologia da ICP. Na próxima seção, discute-se quantitativamente o custo adicional para emissão de certificados aninhados, tanto no que diz respeito à ICPA quanto à ICPAm.

5.2.1 Custo adicional de emissão de certificados

Como foi visto anteriormente, a desvantagem da ICPA é o custo adicional imposto às ACs devido ao número de certificados aninhados a serem emitidos. Nessa seção, será mostrado esse custo de forma analítica para a ICPAm comparado com o da ICPA.

Sejam P_{ICPA} e P_{ICPAm}, definidos pelas Equações 5.1 e 5.2, os fatores de custos adicionais de emissão de certificados aninhados, respectivamente, da ICPA e IPCAm, em que:

- V é o número de certificados tradicionais emitidos em uma ICP;

- V_{ICPA} indica o número de certificados aninhados emitidos pelo conjunto de ACs x em uma ICPA. Por simplicidade, o conjunto formado pela AC A_i será representado apenas por A_i e o conjunto formado por todas as ACs uma ICP, ICPA ou IPCAm será representado por Δ. Logo, $V_{ICPA}(A_i)$ representa todos os certificados aninhados emitidos em uma ICPA por A_i, enquanto $V_{ICPA,}(\Delta)$, por clareza representado simplesmente por V_{ICPA}, representa todos os certificados aninhados emitidos para formar a ICPA;

- $V_{ICPAm}(x)$ é o número de certificados aninhados emitidos pelo conjunto de ACs x em uma ICPAm. Também por clareza, $V_{IPCAm}(\Delta)$ será representado por V_{IPCAm}.

$$\text{P}_{ICPA} = \frac{V_{ICPA} + V}{V} = 1 + \frac{V_{ICPA}}{V} \tag{5.1}$$

$$\text{P}_{ICPAm} = \frac{V_{ICPAm} + V}{V} = 1 + \frac{V_{IPCAm}}{V} \tag{5.2}$$

Considerando uma ICP qualquer, com um conjunto de usuários Θ, o número de certificados tradicionais emitidos na ICPA é igual ao número de caminhos singulares (que possuem apenas um certificado) entre as ACs e os usuários finais e entre as próprias ACS. Sendo V o número de certificados emitidos, pode-se escrever a Equação 5.3, em que NCS() indica o número de caminho singulares.

$$V = \sum_{A_i \,\epsilon\, \Delta} \sum_{A_j \,\epsilon\, \Delta} \text{NCS}(A_i, A_j) + \sum_{A_i \,\epsilon\, \Delta} \sum_{u_j \,\epsilon\, \Theta} \text{NCS}(A_i, u_j) \tag{5.3}$$

Para o exemplo da Figura 5.3, aplicando-se a Equação 5.3,$V = 4m + 8$. Somente as ACs A_2, A_5, A_6 e A_8 possuem caminhos singulares com usuários finais, cada qual com m certificados emitidos, totalizando $4m$. Por outro lado, existem 8 caminhos singulares entre as ACs, como mostrado na Tabela 5.1.

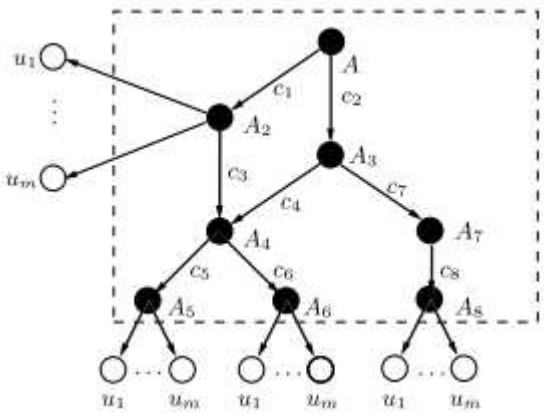


Figura 5.3: ICP exemplo

Origem	Destino	Caminhos	Núm. Certs.
A_1	A_2	c_1	m
	A_3	c_2	0
	A_4	c_1c_3, c_2c_4	0
	A_5	$c_1c_3c_5$, $c_2c_4c_5$	m
	A_6	$c_1c_3c_6$, $c_2c_4c_6$	m
	A_7	c_2c_7	0
	A_8	$c_2c_7c_8$	m
A_2	A_4	c_3	0
	A_5	c_3c_5	m
	A_6	c_3c_6	m
A_3	A_4	c_4	0
	A_5	c_4c_5	m
	A_6	c_4c_6	m
	A_7	c_7	0
	A_8	c_7c_8	m
A_4	A_5	c_5	m
	A_6	c_6	m
A_7	A_8	c_8	m

Tabela 5.1: Caminhos singulares e não singulares para a AC A da Figura 5.3

Para uma ICPA originada de uma ICP qualquer, Levi [19] estabeleceu que o número de certificados aninhados emitidos por A_i ($A_i \epsilon \Delta$), $V_{ICPA}(A_i)$, de forma que exista um um caminho de certificação aninhado para cada caminho de certificação tradicional existente entre A_i e os membros de Θ na ICP, é igual ao número de caminhos não singulares (compostos por mais de um certificado) entre A_i e os membros de Θ, mostrado na Equação 5.4. NCNS() indica o número de caminhos não singulares.

$$\begin{aligned} V_{ICPA}(A_i) &= \sum_{u_j \epsilon \Theta} \text{NCNS}(A_i, u_j) \\ &= \text{NCNS}(A_i, \Theta) \end{aligned} \tag{5.4}$$

O número total de certificados a serem emitidos pelas ACs da ICPA é igual ao número total de caminhos não singulares distintos entre todas as ACs e todos os usuários finais (Equação 5.5).

$$\begin{aligned} V_{ICPA} &= \sum_{A_i \epsilon \Delta} V_{ICPA}(A_i) \\ &= \sum_{A_i \epsilon \Delta} (\sum_{u_j \epsilon \Theta} \text{NCNS}(A_i, u_j)) \\ &= \sum_{A_i \epsilon \Delta} \text{NCNS}(A_i, \Theta) \end{aligned} \tag{5.5}$$

Observa-se que cada caminho (singular ou não-singular) entre duas ACs A_i e A_j, dá origem a um número de caminhos não-singulares entre A_i e os usuários que tiveram certificados emitidos por A_j igual ao número de certificados emitidos para usuários finais por A_j. Por exemplo, para o caminho $c_1c_3c_5$ (Figura 5.3), serão gerados m caminhos não singulares e, consequentemente, deverá haver a emissão de m certificados aninhados por A_i. Logo, pode-se escrever $V_{IPCA}(A_i)$ como mostrado na Equação 5.6, em que que $\text{NCERT}(A_j, \Theta)$ indica o número de certificados emitidos por A_j para usuários finais e $\text{NCS}(A_i, A_j)$ indica o número de caminhos singulares entre A_i e A_j.

$$\begin{aligned} V_{A_i,IPCA} &= \text{NCNS}(A_i, \Theta) \\ &= \sum_{u_j \,\epsilon\, \Theta} \text{NCNS}(A_i, u_j) \\ &= \sum_{A_j \,\epsilon\, \Delta} (\text{NCNS}(A_i, A_j) \times \text{NCERT}(A_j, \Theta)) \\ &\quad + \sum_{A_j \,\epsilon\, \Delta} (\text{NCS}(A_i, A_j) \times \text{NCERT}(A_j, \Theta)), \end{aligned} \tag{5.6}$$

Da Equação 5.5 e da Equação 5.6, pode-se escrever a Equação 5.7:

$$\begin{aligned} V_{ICPA} &= \sum_{A_i \,\epsilon\, \Delta} \text{NCNS}(A_i, \Theta) \\ &= \sum_{A_i \,\epsilon\, \Delta} (\sum_{A_j \,\epsilon\, \Delta} (\text{NCNS}(A_i, A_j) \times \text{NCERT}(A_j, \Theta)) \\ &\quad + \sum_{A_j \,\epsilon\, \Delta} (\text{NCS}(A_i, A_j) \times \text{NCERT}(A_j, \Theta))) \\ &= \sum_{A_i \,\epsilon\, \Delta} (\sum_{A_j \,\epsilon\, \Delta} (\text{NCNS}(A_i, A_j) \times \text{NCERT}(A_j, \Theta))) \\ &\quad + \sum_{A_i \,\epsilon\, \Delta} (\sum_{A_j \,\epsilon\, \Delta} (\text{NCS}(A_i, A_j) \times \text{NCERT}(A_j, \Theta))). \end{aligned} \tag{5.7}$$

Para o exemplo da Figura 5.3, utilizando a Equação 5.6, a partir da Tabela 5.1, obtém-se: $V_{ICPA}(A_1) = 2m + 2m + m + m = 6m$ (ignoraram-se os termos nulos). Para as demais ACs, obtém-se $V_{ICPA}(A_2) = 2m$, $V_{ICPA}(A_3) = 3m$, $V_{ICPA}(A_4) = 2m$ e $V_{ICPA}(A_7) = m$. Logo, $V_{ICPA} = 14m$ e pela Equação 5.1, $\text{P}_{ICPA} = 1 + \frac{14m}{4m+8}$.

O número de certificados aninhados a serem emitidos pela AC A_i da ICPAm é igual ao número de caminho não singulares entre A_i e as demais ACs. O número total de certificados aninhados emitidos numa ICPAm é igual ao número de caminhos não singulares entre as ACs da ICPAm. As Equações 5.8 e 5.9 formalizam o que foi descrito.

$$\begin{aligned} V_{ICPAm}(A_i) &= \sum_{A_j \,\epsilon\, \Delta} \text{NCNS}(A_i, A_j) \\ &= \text{NCNS}(A_i, \Delta) \end{aligned} \tag{5.8}$$

$$\begin{aligned} V_{ICPAm} &= \sum_{A_i \,\epsilon\, \Delta} \left(\sum_{A_j \,\epsilon\, \Delta} \text{NCNS}(A_i, A_j) \right) \\ &= \sum_{A_i \,\epsilon\, \Delta} \text{NCNS}(A_i, \Delta) \end{aligned} \tag{5.9}$$

Por exemplo, na ICP mostrada na Figura 5.3, cujos caminhos são mostrados na Tabela 5.1, há entre a AC A_1 e as demais ACs da ICP, 8 caminhos não singulares. Pela Equação 5.8, $V_{ICPAm}(A_1) = 8$. Ainda observando a Tabela 5.1, vê-se que $V_{ICPAm}(A_2) = 2$, $V_{ICPAm}(A_3) = 3$. Logo, $V_{ICPAm} = 13$. Pela Equação 5.2, $\text{P}_{ICPAm} = 1 + \frac{13}{4m+8}$.

Fazendo-se a divisão $\frac{\text{P}_{ICPA}}{\text{P}_{ICPAm}}$, obtém-se um valor que significa quanto vezes mais a ICPA emite mais certificados do que a IPCAm. No exemplo da Figura 5.3, para $m \gg 1$, essa relação tem valor aproximadamente igual a $4,5m$, ou seja, na ICPA são emitidos $4,5m$ vezes mais certificados aninhados do que na ICPAm (somente para o exemplo acima)[1].

O estabelecimento de uma relação direta entre V_{ICPA} e V_{ICPAm} para uma ICP genérica é uma tarefa difícil, pois ambos os valores dependem da topologia da ICP. A seguir, consideram-se dois casos particulares: um em árvore m-ária, proposto por Levi [19], e outro baseado na estrutura da ICP Brasil [5].

ICP em forma de árvore

Para efeitos de comparação com o trabalho de Levi [19], será feita a análise para o caso particular de uma ICP em forma de árvore m-ária completa. Suponha que esta árvore tenha altura l, em que os nós de altura l são usuários finais e os demais são ACs. Ou seja, apenas as ACs de altura $l-1$ emitem certificados para os usuários finais. As demais apenas emitem certificados para outras ACs.

Para tal árvore, as ACs de nível j, $0 \leq j \leq l-2$, emitem m certificados tradicionais para as ACs de nível $j+1$ e nenhum certificado para usuários finais. Além disso, cada AC de nível $l-1$ somente emite m certificados para usuários finais. O número de nós de altura j é m^j. Logo, o número total de certificados tradicionais emitidos nessa ICP, V, é dado pela Equação 5.10:

[1] $\frac{\text{P}_{ICPA}}{\text{P}_{ICPAm}} = \frac{1+\frac{14m}{4m+8}}{1+\frac{13}{4m+8}} = \frac{18m+8}{4m+21} \approx 4,5m$

$$\begin{aligned} V &= \sum_{A_i \,\epsilon\, \Delta} \sum_{A_j \,\epsilon\, \Delta} \text{NCS}(A_i, A_j) + \sum_{A_i \,\epsilon\, \Delta} \sum_{u_j \,\epsilon\, \Theta} \text{NCS}(A_i, u_j) \\ &= \sum_{j=0}^{l-2} m.m^j + m.m^{l-1} \\ &= \sum_{j=0}^{l-1} m^j.m \\ &= m\frac{m^l - 1}{m - 1}. \end{aligned} \tag{5.10}$$

Na ICPAm, o total de certificados aninhados V_{ICPAm} é dado pela Equação 5.11. Para uma AC de altura (nível) j, existe m^2 caminhos não singulares para as AC de nível $j+2$, m^3 para as de de nível $j+3$ e assim por diante. Para o nível $l-1$, existem m^{l-j-1}, caminhos não singulares. Logo, o número de caminhos não singulares entre uma AC de nível j e as demais ACs da ICP é dado por $\sum_{k=0}^{l-j-1} m^{k+2}$. Além disso existem m^j ACs de nível j. Como o número de certificados aninhados emitidos na ICPAm é igual ao número de caminhos não singulares entre as ACs, pode-se escrever:

$$V_{IPCAm} = \sum_{j=0}^{l-3} m^j \sum_{k=0}^{l-j-3} m^{k+2}. \tag{5.11}$$

O fator de custo adicional de emissão de certificados aninhados na ICPAm, P_{ICPAm} é dado pela Equação 5.12:

$$\begin{aligned} \text{P}_{ICPAm} &= 1 + \frac{V_{ICPAm}}{V} \\ &= 1 + \frac{\sum_{j=0}^{l-3} m^j \sum_{k=0}^{l-j-1} m^{k+2}}{m\frac{m^l-1}{m-1}} \end{aligned} \tag{5.12}$$

Como nessa topologia apenas as ACs de altura $l-1$ emitem certificados para os usuários finais, para encontrar os número de certificados aninhados emitidos na ICPA, V_{ICPA}, devem ser considerados apenas os caminhos que possuem essas ACs. O número de caminhos não singulares entre uma AC de altura j e as de altura $l-1$ é igual a $m^{(l-j-1)}$. Existem m^j ACs de nível j e cada AC de nível $l-1$ emite m certificados para os usuários finais. O número de caminhos singulares é m. Logo:

$$V_{IPCA} = \sum_{j=0}^{l-3} m^j.m^{l-j-1}.m + m^{l-1}.m = (l-1)m^l. \tag{5.13}$$

A Equação 5.14 define o custo adicional de emissão de certificados aninhados na ICPA, P_{ICPA}. Isto é, o fator que indica a relação entre o total de certificados emitidos na ICPA (aninhados e tradicionais) e o número de certificados tradicionais emitidos na ICP que deu origem à ICPA.

$$\begin{aligned} \mathrm{P}_{ICPA} &= 1 + \frac{V_{IPCA}}{V} \\ &= 1 + \frac{(l-1)m^l}{m\frac{m^l-1}{m-1}} \end{aligned} \tag{5.14}$$

Os gráficos das Figuras 5.4 e 5.5 mostram o comportamento do custo adicional de certificação (P) em função do número de nós (m) para, respectivamente, a ICPA e ICPAm. Foram utilizados diferentes valores de l, indicados nos gráficos.

Da análise dos gráficos têm-se as seguintes conclusões:

- o custo adicional de certificação da ICPA é maior que o da ICPAm. Enquanto para a ICPA o custo adicional de certificação se aproxima de l, o da ICPAm se aproxima de 1;
- o custo adicional de certificação da ICPA aumenta com o aumento do número de nós, enquanto que na ICPAm ocorre o contrário.

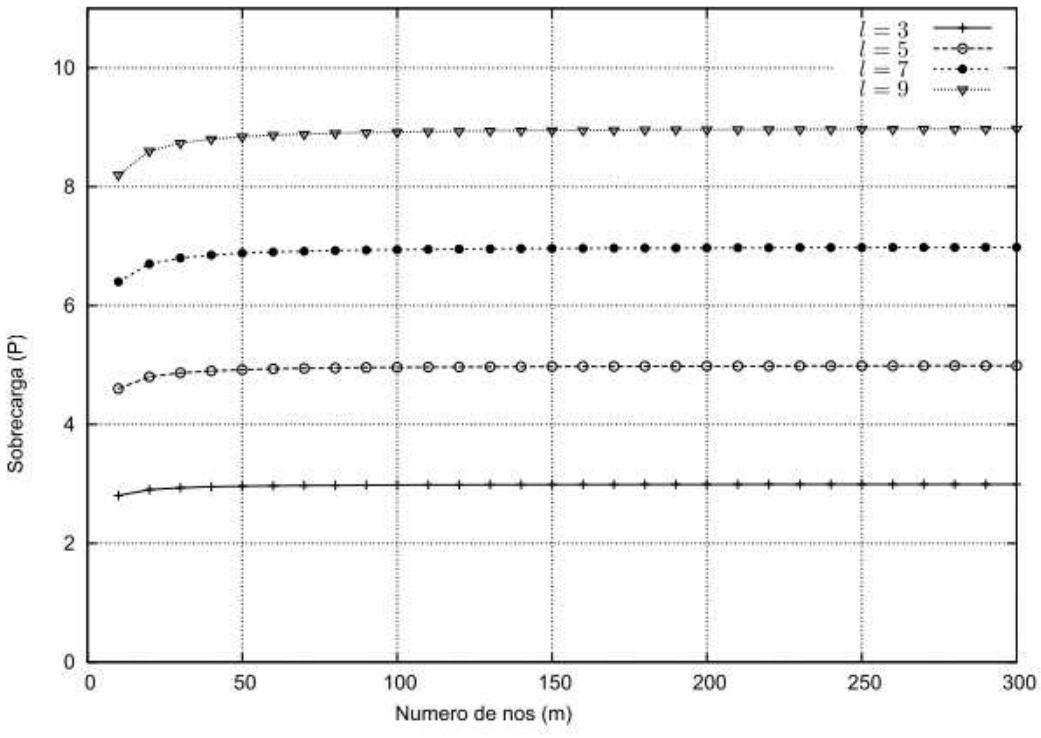


Figura 5.4: Número de nós versus custo adicional de certificação - ICPA

ICP Brasil

A medida provisória 2.200-2, de 24 de agosto de 2001, cria a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), composta por uma autoridade gestora de políticas (CG),

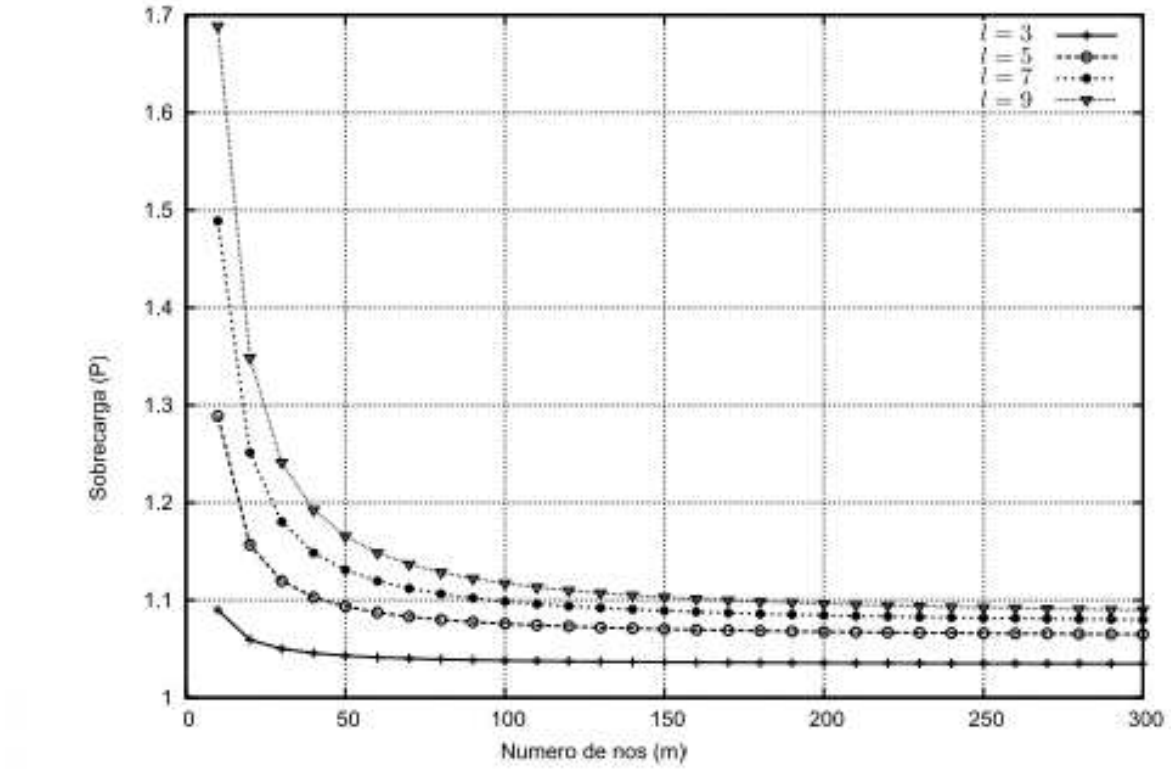


Figura 5.5: Número de nós versus custo adicional de certificação - ICPAm

por uma cadeia de autoridades certificadoras que inclui a Autoridade Certificadora Raiz e autoridades certificadoras e autoridades de Registro.

A estrutura atual da ICP-Brasil é mostrada na Figura 5.6. Nesse cenário, o número de certificados aninhados emitidos para formar a ICPAm é 14 ($V_{ICPAm} = 14$), independente do número de usuários. Como foi visto anteriormente, esse é o número de caminhos não singulares entre as ACs. Observe que todos os caminhos não singulares são entre a AC raiz e suas ACs netas.

Para determinar o número de certificados tradicionais e o número de certificados aninhados emitidos na ICPA deve-se conhecer o número de usuários finais e sua distribuição pela ICP. Como não se tem tal informação, para efeitos de comparação, supõem-se que ACs intermediárias (que emitem certificados para outras ACs) não emitem certificados para usuários finais (A AC raiz é proibida de realizar tal operação por lei) e que as demais ACs emitem m certificados para usuários finais. A Figura 5.6 mostra tal configuração.

Para a ICP mostrada na Figura 5.6, $V = 16m + 21$ e $V_{ICPA} = 30m$. Consequentemente $\mathrm{P}_{ICPA} = 1 + \frac{30m}{16m+21}$ e $\mathrm{P}_{ICPAm} = 1 + \frac{12}{16m+21}$. Para valores grandes de m, por exemplo, $m > 1000$, $\mathrm{P}_{ICPA} \approx 1 + \frac{30m}{16m} \approx 2.87$. Ou seja, há um aumento de aproximadamente 187% na emissão de certificados numa ICPA. Por outro lado, o custo adicional de emissão de certificados aninhados para uma ICPAm é $V_{ICPAm} \approx 1$. Isso significa que o custo de emissão dos certificados aninhados, para esse caso, é praticamente irrelevante na ICPAm.

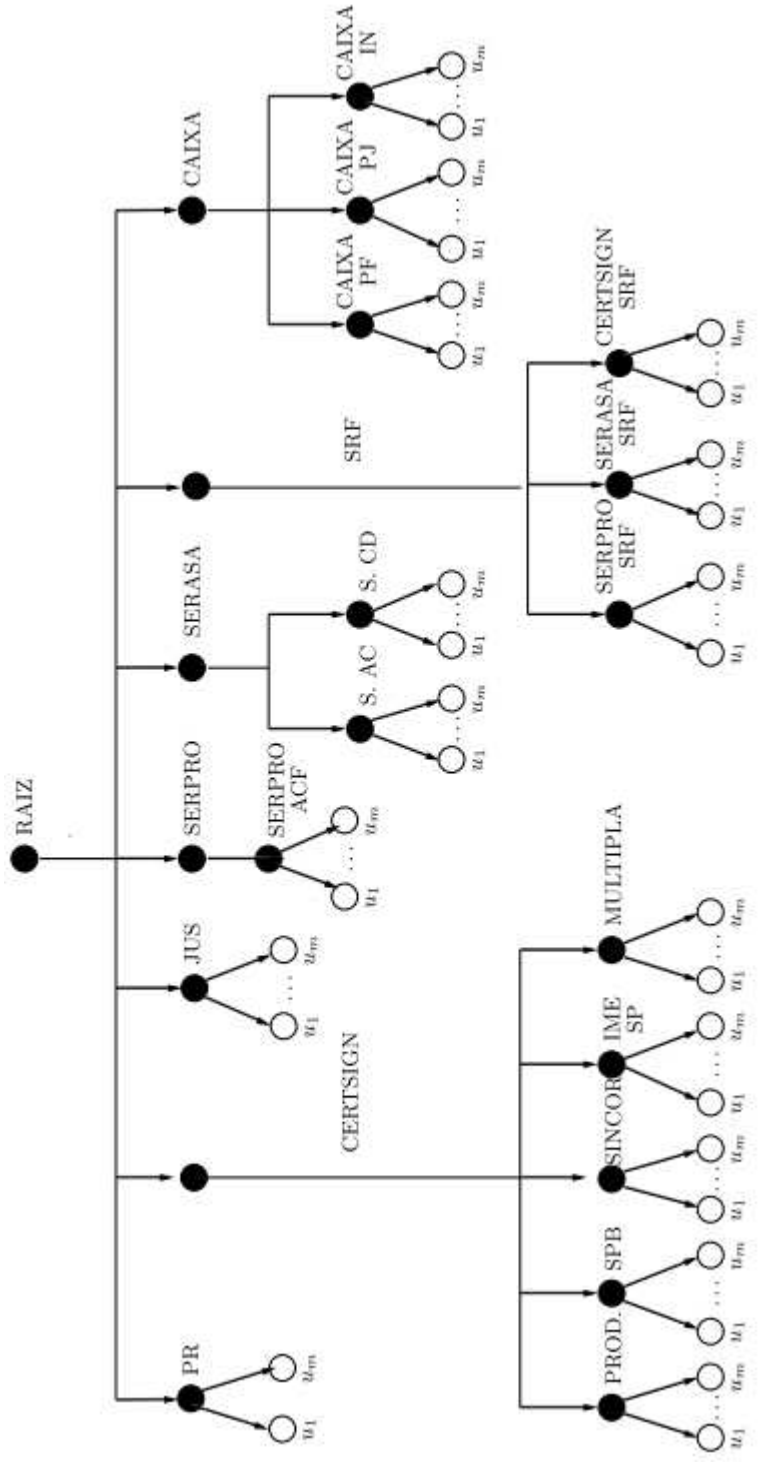


Figura 5.6: Estrutura da ICP-Brasil

Capítulo 6

Conclusões e trabalhos futuros

Durante este trabalho foram analisados vários mecanismos de validação de certificados, principalmente no que tange aos custos de transmissão e de processamento. No Capítulo 4, apresentaram-se os mecanismos de validação e os seus respectivos custos de validação para um caminho de certificação. Observando os mecanismos propostos, vê-se que um recurso muito utilizado para reduzir os custos de validação é substituir operações de criptografia assimétricas (assinaturas digitais e verificação de assinaturas digitais) por operações de resumo, que requerem menos processamento e têm como resultado sequências de bits menores, o que resulta em custos de transmissão menores. Isso ocorre no NOVOMODO, CRT/2-3CRT, EFFECT e principalmente na ICPA/ICPAm.

Como foi visto, quando se considera um caminho de certificação com vários certificados, a ICPA apresentou o menor custo de processamento do verificador e custo de transmissão do verificador muito perto dos certificados efêmeros, que têm os menores custos nesse quesito. A grande desvantagem da ICPA é custo de processamento do ASR para emitir os certificados aninhados. Dependendo da topologia e do número de usuários do ambiente considerado, viu-se que ela pode se tornar inviável. Além disso, a ICPA também tem limitações no aspecto administrativo, principalmente pelo fato das ACs estarem diretamente envolvidas na emissão de certificados para usuários finais pelas suas ACs descendentes. Também deve-se notar que o ganho fornecido pela ICPA será tanto maior quanto maior for o caminho de certificação. Tal característica é interessante, uma vez que a integração de ICPs já existentes, como no caso americano, tende a criar caminhos de certificação cada vez maiores. Outro ponto que deve ser notado é que a ICPA/ICPAm não substituem os esquemas tradicionais de validação de certificados, mas contribuem para que o processo de validação seja feito de forma mais eficiente.

No sentido de contornar as limitações da ICPA, foi proposta a ICPAm, que remove a necessidade das ACs estarem diretamente envolvidas na emissão de certificados para usuários finais pelas suas ACs descendentes. Como consequência disso, há redução significativa dos custos de emissão de certificados aninhados (Capítulo 5), tornando a ICPAm mais escalável e flexível do que a ICPA. Uma desvantagem da modificação proposta é o aumento do custo de processamento do verificador, pois é necessária uma operação a mais de verificação de assinatura digital (ver 5.2). No entanto, esse custo é aceitável, pois torna a ICP mais flexível e escalável. Em especial, a ICPAm pode ser utilizada mesmo quando há certificação cruzada.

Embora muitos mecanismos tenham sido propostos para a validação de certificados, geralmente bem mais eficientes do que as LCRs, ainda há uma forte resistência a esses mecanismos. Grande parte das aplicações tem optado por manter o uso de LCRs, por exemplo, a ICP-Brasil, com uma janela de vulnerabilidade de aproximadamente 3 meses (AC raiz). Mesmo o OCSP, também padronizado pela IETF, ainda não tem grande aceitação.

Outra questão é que o processo de validação de certificados, embora teoricamente bem definido e completo, não tem sido assim na prática. Por exemplo, em geral, os usuários não verificam as LCRs e sujeitam-se a utilizarem certificados revogados, embora elas sejam disponibilizadas. Em outros casos, os usuários são induzidos a acreditarem em autoridades certificadoras que eles sequer sabem que existem: os atuais navegadores possuem uma lista de ACs pré-determinadas. O usuário geralmente não conhece as ACs que estão nessa lista e, em alguns casos, não sabe nem mesmo que tal lista existe, embora confie em certificados emitidos por tais ACs.

Trabalhos futuros

Uma questão interessante que pode ser abordada futuramente é analisar detalhadamente como os certificados aninhados poderiam ser utilizados sob a ótica administrativa, principalmente para o controle do estabelecimento de caminhos de certificação. Na forma como os certificados aninhados foram emitidos (ICPA/IPCAm) não é possível estabelecer um controle dos caminhos de certificação, pois, embora os certificados aninhados não permitam que tais caminhos sejam criados, os tradicionais o fazem. Uma possibilidade que merece estudo é uma abordagem em que somente certificados aninhados seriam emitidos para ACs. Logo, não haveria caminhos tradicionais entre ACs, mas somente caminhos aninhados, cujo último certificado seria um certificado tradicional e auto assinado pela AC. Aparentemente, tal arquitetura permitiria um controle muito mais refinado dos caminhos de autenticação, sem modificar o modo como os certificados seriam validados em relação à ICPAm.

Referências Bibliográficas

[1] Secure hash standard. Technical Report FIPS PUB 180-1, National Institute of Standards and Technology - NIST, 1993.

[2] Data encryption standard - DES. Technical Report FIPS PUB 46-3, National Institute of Standards and Technology - NIST, 1999.

[3] Digital signature standard - DSS. Technical Report FIPS PUB 186-2, National Institute of Standards and Technology - NIST, 2000.

[4] Advanced encryption standard - AES. Technical Report FIPS PUB 197, National Institute of Standards and Technology - NIST, 2001.

[5] Medida provisória n.o 2.200-2, de 24 de agosto de 2001. Technical report, Presidência da República do Brasil, 2001.

[6] PKCS 1: RSA cryptography standard. Technical Report Versão 2.1, RSA Laboratories, 2002.

[7] Carlisle Adams and Steve Lloyd. *Understanding PKI:Concepts, Standards and Deployment Considerations*. Addison-Wesley, third edition, 2003.

[8] William Aiello, Sachin Lodha, and Rafail Ostrovsky. Fast digital identity revocation (extended abstract). In *CRYPTO '98: Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*, pages 137–152, London, UK, 1998. Springer-Verlag.

[9] Andre Arnes. Public key certificate revocation schemes. Master's thesis, Norwegian University of Science and Tecnology, 2000.

[10] David A. Cooper. A model of certificate revocation. In *ACSAC '99: Proceedings of the 15th Annual Computer Security Applications Conference*, page 256, Washington, DC, USA, 1999. IEEE Computer Society.

[11] D. Coppersmith and M. Jakobsson. Almost optimal hash sequence traversal. In *Financial Cryptography '02*, 2002.

[12] Carl M. Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian Thomas, and Tatu Ylonen. Rfc 2693 - SPKI certificate theory. Technical report, Network Working Group, 1999.

[13] Trevor Freeman, Russell Housley, Ambarish Malpani, David Cooper, and Tim Polk. Standard certificate validation protocol - SCVP. Technical report, IETF PKIX Working Group, 2006.

[14] Irene Gassko, Peter Gemmell, and Philip D. MacKenzie. Efficient and fresh cerification. In *PKC '00: Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography*, pages 342–353, London, UK, 2000. Springer-Verlag.

[15] Russell Housley, W. Polk, W. Ford, and Dave Solo. Internet x.509 public key infrastructure, certificate and CRL profile. Technical report, IETF PKIX Working Group, 2002.

[16] Markus Jakobsson. Fractal hash sequence representation and traversal. In *Proceedings of the 2002 IEEE International Symposium on Information Therory (ISIT '02)*, pages 437–444, 2002.

[17] Paul C. Kocher. On certificate revocation and validation. In *Proceedings of the Second International Conference on Financial Cryptography*, pages 172–177, 1998.

[18] Loren M. KohnFelder. Towards a practical public-key cryptosystem. Master's thesis, Massachusetts Institute of Technology, 1978.

[19] Albert Levi. *Design and Performance Evaluation of the Nested Certification Scheme and its Applications in Public Key Infrastructures.* PhD thesis, Bogazici University, 1999.

[20] Albert Levi, M. Ufuk Çaglayan, and Çetin Kaya Koç. Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure. *ACM Trans. Inf. Syst. Secur.*, 7(1):21–59, 2004.

[21] Wenbo Mao. *Modern Cryptography: Theory and Practice.* Prentice Hall PTR, 2003.

[22] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[23] Ralph Merkle. *Secrecy, Authentication, and public key systems.* PhD thesis, 1979.

[24] Silvio Micali. Enhanced certificate revocation. Technical Report MIT/LCS/TM-542, Massachusetts Institute of Technology, 1995.

[25] Silvio Micali. Efficient certificate revocation. Technical Report MIT/LCS/TM-542b, Massachusetts Institute of Technology, 1996.

[26] Silvio Micali. Novomodo scalable certificate validation and simplified PKI management. In *1st Annual PKI Research Workshop*, pages 15–25, 2002.

[27] Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. X.509 internet public key infrastructure online certificatestatus protocol - OCSP. Technical report, IETF PKIX Working Group, 1999.

[28] Moni Naor and Kobbi Nissim. Certificate revocation and certificate update. In *Proceedings 7th USENIX Security Symposium (San Antonio, Texas)*, 1998.

[29] Rebecca Nielsen. Observations from the deployment of a large scale PKI. In *Online Proceedings 4th Annual PKI R&D Workshop*, 2005.

[30] Denis Pinkas and Russell Housley. RFC 3379: Delegated path validation and delegated path discovery protocol requirements. Technical report, IETF PKIX Working Group, 2002.

[31] Ronald L. Rivest. Can we eliminate certificate revocations lists? In *Financial Cryptography*, pages 178–183, 1998.

[32] Ronald. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 26(1):96–99, 1983.

[33] Douglas Stinson. *Cryptography: Theory and Practice*. CRC Press, 1995.