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

Martín Augusto Gagliotti Vigil

INFRAESTRUTURA DE CHAVES PÚBLICAS OTIMIZADORA

Florianópolis
2010

Martín Augusto Gagliotti Vigil

INFRAESTRUTURA DE CHAVES PÚBLICAS OTIMIZADORA

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

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis
2010

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

V677i Vigil, Martín Augusto Gagliotti
Infraestrutura de chaves públicas otimizadora [dissertação] / Martín Augusto Gagliotti Vigil ; orientador, Ricardo Felipe Custódio. - Florianópolis, SC, 2010.
94 p.: il., grafs., tabs.

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

Inclui referências

1. Ciência da computação. 2. Assinaturas digitais. 3. Documentos eletrônicos. 4. Infraestrutura de chaves públicas. I. Custodio, Ricardo Felipe. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. III. Título.

CDU 681

Martín Augusto Gagliotti Vigil

INFRAESTRUTURA DE CHAVES PÚBLICAS OTIMIZADORA

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

Florianópolis, 20 de Agosto de 2010

Mário Antônio Ribeiro Dantas, Dr.
Coordenador do Curso

Banca Examinadora:

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

Prof. Eugene Francis Vinod Rebello, Dr.
Universidade Federal Fluminense

Prof. Roberto Samarone dos Santos Araújo, Dr.
Universidade Federal do Pará

Prof. Ricardo Alexandre Reinaldo de Moraes, Dr.
Universidade Federal de Santa Catarina

Prof. Lau Cheuk Lung, Dr.
Universidade Federal de Santa Catarina

Aos meus pais e avós pela dedicação para que seus descendentes sejam pessoas mais instruídas, livres e felizes.

AGRADECIMENTOS

Aos meus pais, José Luiz e María Inés, pela dedicação, carinho e imparcialidade na criação que eu e minhas irmãs recebemos. Esta dissertação é apenas uma das consequências de um trabalho de cidadania de meus pais, cujo objetivo é que seus filhos sejam pessoas ricas de espírito e de conhecimento bem como cidadãos que venham a melhorar esta nação.

Ao orientador desta dissertação, professor Ricardo Felipe Custódio, pela confiança e, consequemente, pelas oportunidades que me foram dadas ao longo desses 5 anos de trabalho e aprendizado. Agradeço muito pelos ensinamentos e conselhos, em especial aqueles que ultrapassaram os limites deste trabalho e que me guiaram para decisões certas.

Ao co-orientador desta dissertação, professor Ricardo Alexandre Reinaldo de Moraes, pelos ensinamentos e sugestões que enriqueceram este trabalho e os artigos científicos que publiquei. Sem dúvida, devo ao Ricardo grande parte do que aprendi sobre organização e escrita de trabalhos acadêmicos.

Ao Nelson da Silva por críticas que foram fundamentais no amadurecimento do tema deste trabalho. Agradeço também por ceder seu trabalho inicial sobre estimativa de esforços computacionais, o qual foi estendido neste trabalho.

Aos alunos de graduação Deise Luise Wrasse, Lucas Silveira e Khristian Shönrock, cujas contribuições permitiram-me alcançar os objetivos deste trabalho. Adicionalmente, tais alunos me proporcionaram minha primeira experiência de docência, em que pude repassar parte dos conhecimentos que adquiri no LabSEC.

Aos antigos colaboradores do LabSEC, Jean Everson Martina, Túlio Cícero Salvaro de Souza e Marcelo Carlomagno Carlos pelos ensinamentos durante meus primeiros anos no LabSEC. Agradeço ao Jeandré Monteiro Sutil pelas frequentes sugestões para este e outros trabalhos, como ainda pelo companheirismo e grande amizade tanto no LabSEC quanto no Mar. Agradeço também aos demais colaboradores do LabSEC pela cooperação e amizade que tornam meus dias de trabalho mais felizes!

À minha namorada Karina Bettega Felipe, a quem tomo como exemplo de esforço e dedicação profissional. Agradeço não só pelo carinho, amizade e alegria em todos os momentos, como também pela sua

experiência e conselhos na elaboração deste trabalho.

Por fim, agradeço às instituições Financiadora de Estudos e Projetos (FINEP), Instituto Nacional de Tecnologia da Informação (ITI), Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Colégio Notarial do Brasil (CNB) e Câmara Brasileira de Comércio Eletrônico (Camera-e.net). Graças a elas pude me dedicar plenamente ao LabSEC e realizar um trabalho da melhor forma possível.

"Mergulhe no meio das coisas, suje as mãos, caia de joelhos e, então, procure alcançar as estrelas". John. L Curcio

RESUMO

Este trabalho tem como objetivo propor e implementar um novo conceito de certificado: o Certificado Otimizado, base da Infraestrutura de Chaves Públicas Otimizadora. Trata-se de adaptações ao padrão X.509 para reduzir o esforço computacional necessário ao uso de documentos eletrônicos assinados sem a perda da compatibilidade com as aplicações existentes. Tal redução incide na verificação de assinaturas digitais, pois o Certificado Otimizado: (1) dispensa verificação de situação de revogação; (2) substitui carimbos do tempo sobre uma assinatura digital; (3) é emitido por uma Autoridade Certificadora cuja situação de revogação é aferida através do método Novomodo; e (4) possui um caminho de certificação curto. Esta proposta também explora a substituição de Certificados Otimizados quando da obsolescência dos algoritmos criptográficos, tornando possível a manutenção da autenticidade de assinaturas digitais sem o aumento contínuo dos recursos computacionais utilizados. Desta forma, beneficia diretamente verificadores de assinaturas digitais e entidades arquivísticas, as quais enfrentam o desafio de armazenar e manter válidas assinaturas digitais sobre documentos eletrônicos sem demandar quantidades impraticáveis de recursos computacionais. A solução proposta é comparada com o certificado X.509 convencional através da simulação de um cenário de documentos eletrônicos assinados na ICP-Brasil. Os resultados da simulação demonstram que o Certificado Otimizado proporciona uma economia superior a 80% de recursos computacionais ao longo dos anos. Ainda, observa-se, através de testes realizados sobre a implementação do algoritmo *Certificate Path Processing*, presente na Máquina Virtual Java, que o Certificado Otimizado é aderente ao padrão X.509 e, portanto, compatível com a maioria das aplicações de certificação digital existentes. Sem dúvida, tais características tornam o Certificado Otimizado uma atraente solução para reduzir os recursos computacionais necessários no uso de documentos eletrônicos assinados.

Palavras-chave: X.509, Infraestrutura de Chaves Públicas, assinatura digital, documento eletrônico assinado, Novomodo.

ABSTRACT

This work deals with the proposal and the implementation of a new digital certificate concept: an Optimized Certificate, on which Optimizer Public Key Infrastructure is based. This concept implies some changes in the X.509 standard as a means to cut down on the computational effort required to use digital signatures on electronic documents, while keeping compatibility with existing applications. This reduction can be noted when verifying digital signatures because an Optimized Certificate: (1) dismisses the need to verify the revocation status; (2) replaces timestamps for a signature; (3) is issued by a Certification Authority whose revocation status is checked using Novomodo; and (4) presents a short certification path. Also, this proposal takes advantage of replacing an Optimized Certificate before cryptographic algorithms become weak, which makes it possible to maintain authentic digital signatures without requiring an ever-growing amount of computational resources. Therefore, Optimized Certificates benefit the verifiers of digital signatures and archiving entities, which have to overcome the challenge of storing and maintaining valid digital signature on electronic documents within computational resource constraints. The proposal is compared with the conventional X.509 certificate, considering the simulation of a scenario of signed electronic documents in ICP-Brasil. The result of this comparison reveals that an Optimized Certificate can lead to the reduction of computational resources along years at rates above 80%. Moreover, successful tests on the implementation of Certificate Path Processing available in Java Virtual Machine indicate that an Optimized Certificate adheres to X.509 and therefore, with regard to digital signatures, it is compatible with most existing applications. Indeed, such characteristics make Optimized Certificates an attractive solution to reduce the computational resources required for using signed electronic documents.

Keywords: X.509, Public Key Infrastructure, digital signature, signed electronic document, Novomodo.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
ACCO	Autoridade Certificadora de Certificados Otimizados
ACT	Autoridade de Carimbo do Tempo
ASN.1	*Abstract Syntax Notation One*
CAdES	*CMS Advanced Electronic Signatures*
CMS	*Cryptographic Message Syntax*
CO	Certificado Otimizado
CRS	*Certificate Revocation Status*
DER	*Distinguished Encoding Rules*
DVCS	*Data Validation and Certification Server Protocol*
ERS	*Evidence Record Syntax*
ETSI	*European Telecommunications Standards Institute*
HTTP	*Hypertext Transfer Protocol*
ICP	Infraestrutura de Chaves Públicas
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ICPO	Infraestrutura de Chave Pública Otimizada
LabSEC	Laboratório de Segurança em Computação
LCR	Lista de Certificados Revogados
MVJ	Máquina Virtual Java
OCSP	*Online Certificate Status Protocol*
OCSP-X	OCSP *Extensions*
PKCS#7	*Public Key Cryptography Standards #7*
RDN	*Relative Distinguished Name*
SCVP	*Simple Certificate Validation Protocol*
SPKI	Infraestrutura Simples de Chaves Públicas
XAdES	*XMLdSIG Advanced Digital Signatures*
XML	*Extensible Markup Language*
XMLdSig	*XML-Signature Syntax and Processing*

SUMÁRIO

1 INTRODUÇÃO

Recentemente se tem observado a sociedade moderna convergir para o uso de meios eletrônicos e *online* para realizar tarefas do dia-a-dia. Por exemplo, muitos preferem fazer compras e pagar contas pela Internet ao invés de irem pessoalmente a lojas e bancos. Seguindo essa tendência, empresas e instituições governamentais também estão adotando sistemas *online* como meio de reduzir custos, evitar erros humanos e acelerar processos. Por exemplo, podem-se citar as iniciativas norte-americana [1, 2] e brasileira [3, 4] em utilizar documentos eletrônicos de forma a reduzir a retenção de papéis em agências governamentais e tribunais.

Por outro lado, na ausência de contato visual entre as partes envolvidas em sistemas computacionais *online* vê-se a necessidade de mecanismos de segurança. Por exemplo, autenticação dos participantes, garantia de integridade para os dados recebidos e enviados, sigilo e irretratabilidade. Tais requisitos de segurança têm sido satisfatoriamente atendidos por sistemas computacionais baseados em assinaturas digitais [5] e Infraestrutura de Chaves Públicas (ICP) [6]. Infelizmente, utilizar os serviços de uma ICP é uma tarefa complexa, sendo até mesmo inviável em muitos ambientes. Por exemplo, a manutenção a longo prazo da autenticidade de documentos assinados exige uma quantidade sempre crescente de recursos computacionais. Outro exemplo refere-se a redes industriais semfio e a sistemas embarcados, que normalmente não dispõem de recursos computacionais suficientes para usufruir das funcionalidades de uma ICP [7, 8, 9, 10].

Imprescindível em diversos ambientes baseados em ICP, a verificação da autenticidade, integridade e irretratabilidade de documentos eletrônicos assinados consiste em validar a assinatura digital e o certificado de chave pública do signatário [11]. Esse processo demanda recursos computacionais em abundância, pois inclui tarefas complexas, como a busca e a validação de certificados digitais. Além disso, recomendam-se considerar as informações de revogação de certificado, que podem ser obtidas através de consultas externas, por exemplo, para acessar repositórios na web. Tais consultas estão sujeitas a eventuais problemas de comunicação, como baixa velocidade de transferência de dados ou mesmo impossibilidade de conexão. Vale citar ainda que carimbos do tempo [12] são necessários para garantir uma referência temporal confiável ao processo de validação de assinatura digital. Contudo, carimbos do tempo também são documentos eletrônicos assinados e, portanto, dificultam ainda mais a validação de conteúdos assinados.

Não obstante, Martinez-Peláez et al [13] afirma que o volume dos dados de validação - certificados, informações de revogação e carimbos do tempo - é diretamente proporcional à dificuldade da verificação de uma assinatura digital. Com base nesta afirmação, encontram-se publi-

cados diversos trabalhos que buscam reduzir a complexidade do uso de ICPs. Primeiramente estão os certificados aninhados [14], cuja proposta consiste em reduzir a quantidade de validações de certificados em um cadeia de certificação. Em seguida, há os que defendem eliminar de ICPs a revogação de certificados, como propõe Rivest através dos certificados de curta duração [15]. Por fim, destaca-se o trabalho de Micali [16], que apresenta um eficiente sistema de revogação: o método Novomodo.

Baseado nas publicações acima citadas, este trabalho propõe uma solução para facilitar a verificação de assinaturas digitais sobre documentos eletrônicos: o Certificado Otimizado, base da Infraestrutura de Chaves Públicas Otimizadora. Trata-se de um certificado de curta duração adaptado para que sua autenticidade seja facilmente verificada pois: (a) é desnecessário verificar sua situação de revogação; (b) seu caminho de certificação é reduzido e faz uso do eficiente método Novomodo; e (c) substitui carimbos do tempo sobre a assinatura.

Um passo a frente dos trabalhos anteriores, o Certificado Otimizado simplifica também a manutenção a longo prazo da autenticidade da assinatura digital sobre documentos eletrônicos. Através de substituições de Certificados Otimizados obsoletos é possível estender a autenticidade sem, em contra-partida, aumentar o volume de dados de validação e, consequentemente, os esforços computacionais. Para estes apresentam-se estimativas, que são úteis para comparar certificados tradicionais e otimizados.

1.1 OBJETIVOS

Uma das alternativas para a complexidade do uso de serviços de ICP é adaptar os sistemas computacionais, incrementando recursos. Por exemplo, aumentar o poder de processamento e armazenamento. Por outro lado, acredita-se ser possível simplificar o uso da ICP, repensando seus serviços. Essa solução é, sem dúvida, atraente, haja vista que não exige custos para modificar os sistemas atuais.

Desta maneira, o objetivo deste trabalho é apresentar uma nova abordagem para facilitar a verificação e a manutenção a longo prazo da autenticidade de documentos assinados. A abordagem utilizada visa reduzir e manter constante o volume de dados de validação para assinaturas digitais sobre documentos eletrônicos.

1.1.1 Objetivos Específicos

Este trabalho possui os seguintes objetivos específicos:

a) apresentar os conceitos envolvidos e os desafios encontrados na certificação digital de documentos eletrônicos;

b) apresentar trabalhos que busquem solucionar as dificuldades para o uso do serviços de Infraestrutura de Chaves Públicas;

c) apresentar a definição da Infraestrutura de Chaves Públicas Otimizadora (ICPO);

d) descrever um esquema de revogação eficiente para ICPO baseado no método Novomodo;

e) descrever a aplicação do Certificado Otimizado em um domínio de usuários que fazem uso de documentos eletrônicos assinados;

f) implementar um protótipo capaz de utilizar o Certificado Otimizado em documentos eletrônicos assinados;

g) apresentar uma proposta de estimativa de esforços computacionais para o uso de documentos eletrônicos assinados;

h) avaliar a ideia proposta neste trabalho, comparando as certificações digitais convencional e otimizada através de testes sobre um protótipo, de simulações e de estimativas de esforços computacionais.

1.2 MOTIVAÇÃO

São inúmeros os benefícios da desmaterialização de documentos e a substituição de assinaturas manuscritas por digitais. Podem-se citar, por exemplo, fatores ecológicos e a prevenção de diversas fraudes possíveis em documentos em papel. Não obstante, percebe-se que a convergência a documentos eletrônicos assinados ocorre de maneira lenta, fato devido ao uso complexo da ICP, bem como a forma em que esta foi concebida [17].

Nesse contexto, o presente trabalho almeja simplificar tanto a verificação quanto a manutenção da autenticidade de documentos eletrônicos assinados. Assim, pretende-se que os usuários comuns usufruam em larga escala de serviços de ICP bem como que entidades arquivísticas sejam capazes de manter, eficientemente, grandes volumes de documentos eletrônicos assinados.

1.3 HISTÓRICO DOS CERTIFICADOS OTIMIZADOS

A proposta inicial de Certificados Otimizado foi concebida durante o doutoramento de Adriana Elissa Notoya. A nova ideia de certificação otimizada foi apresentada através do trabalho [18] durante o *VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais* (SBSeg), ocorrido no Rio de Janeiro (RJ) em 2007.

Em seguida, o tema foi assumido pelo autor desta dissertação de mestrado. Nessa etapa, publicou-se o trabalho [19] no *5th European PKI Workshop: Theory and Practice* (EuroPKI), ocorrido em Trondheim, Noruega, em 2008. Por fim, com base em correções de vulnerabilidades e melhoramentos, publicou-se o trabalho [20] no SBSEG 2009, corrido em Campinas (SP).

Vale citar também que a pesquisa sobre Certificados Otimizados foi efetuada através de um projeto desenvolvido no Laboratório de Segurança em Computação (LabSEC). Tal projeto contou com a colaboração dos seguintes alunos de graduação em Ciências da Computação e Sistemas de Informação: Deise Luise Wrasse, Glauco Israel Rebello Bondan, Khristian Alexander Schönrock, Leonardo Schmitz da Costa e Lucas Silveira. Eles participaram de uma equipe de desenvolvimento cujo objetivo foi a criação de protótipos para: (a) Autoridade Certificadora Otimizadora; (b) gestor de informações de revogação do método Nomovodo; e (c) aplicação para assinatura digital e otimização de documentos eletrônicos. Por fim, a participação desses alunos produziu os trabalhos de conclusão de curso [21] e [22].

1.4 CONTRIBUIÇÕES

O autor deste trabalho, cuja elaboração norteou-se pelos objetivos citados na Seção 1.1, é diretamente responsável pelas seguintes contribuições:

- descrição dos fatores que dificultam o uso de documentos eletrônicos assinados;
- estimativa para o esforço computacional inerente à verificação e à manutenção da autenticidade a longo prazo de documentos eletrônicos assinados;
- proposta de uma nova abordagem para simplificar a verificação e a manutenção da autenticidade a longo prazo de documentos eletrônicos assinados;
- implementação da proposta anteriormente citada através de um novo serviço acrescentado a uma ICP;
- adaptação do método de revogação Novomodo para que este possa ser utilizado por uma âncora de confiança (i.e. AC Raiz), sem que esta seja exposta nem tenha seus custos operacionais incrementados;
- proposta de uma nova abordagem de carimbo do tempo relativo, a qual é integrada com o método Novomodo e pode ser utilizada para auditoria sobre emissão de certificados digitais;

1.5 LIMITAÇÕES DO TRABALHO

O escopo deste trabalho restringe-se apenas ao padrão X.509, mesmo havendo outras abordagens de Infraestrutura de Chaves Públicas (ICP), tais como *Simple Public Key Infrastructure* [23, 24] e *Pretty Good*

Privacy [25]. Ainda, o trabalho limita-se a adicionar um novo serviço – a Autoridade Certificadora de Certificados Otimizados – a uma ICP sem modificar o padrão X.509.

Embora este trabalho aborde a simplificação da verificação de documentos eletrônicos assinados, ele limita-se apenas à redução do volume dos dados de validação para assinaturas digitais. Também, não se aborda a eficiência de diferentes algoritmos criptográficos utilizados na certificação digital.

Semelhante a verificação, a manutenção da autenticidade a longo prazo de documentos eletrônicos assinados limita-se a manter constante o volume dos dados de validação. Portanto, este trabalho não aborda outras técnicas comuns para o arquivamento a longo prazo de conteúdos digitais, tais como transformações de formatos (e.g. [26]) e sigilo (e.g. [27]).

1.6 METODOLOGIA E ORGANIZAÇÃO DO TRABALHO

Para se alcançarem os objetivos deste trabalho, iniciou-se pelo estudo de artigos, normas e relatórios técnicos a respeito de: a) otimização da ICP; b) esquemas de revogação de certificados; c) formatos de assinatura digital; e d) manutenção a longo prazo da autenticidade de documentos assinados. Tais materiais foram classificados de acordo com os problemas que pretendiam tratar. Após a escolha e classificação dos materiais pertinentes a este trabalho, selecionaram-se aqueles úteis para a fundamentação da proposta sobre Infraestrutura de Chaves Públicas Otimizadora (ICPO).

Em seguida, elaboraram-se as definições conceituais da ICPO e do Certificado Otimizado (CO). Esses conceitos foram discutidos dentro de um grupo de pesquisa, o qual contribuiu para o aprimoramento deles. Ainda, publicaram-se artigos sobre o tema em conferências de segurança em informação para verificar a aceitação do meio científico e colher críticas que pudessem proporcionar melhorias ao trabalho.

Dada a dificuldade de definir formalmente a ICPO, optou-se por implementar um protótipo capaz de testar a solução proposta. Portanto, desenvolveu-se uma aplicação em Java capaz de empregar o CO em documentos eletrônicos assinados, bem como verificar a autenticidade destes. O resultados dos testes foram analisados e utilizados como fundamento para avaliar a solução.

Uma vez consolidadas as definições da ICPO e do CO, estimaram-se os esforços computacionais do uso do CO a longo prazo em documentos eletrônicos assinados. Tal estimativa baseou-se na observação da quantidade de assinaturas digitais a serem verificadas bem como a capacidade de armazenamento necessária para manter tanto o documento eletrônico assinado e as evidências de validade da assinatura digital.

Finalmente, com base nos resultados das etapas anteriores, elaboraram-se as conclusões. Estas contemplam a consolidação da solução, as vantagens decorrentes de seu uso bem como trabalhos futu-

ros.

Este documento, que contempla as etapas acima citadas, é organizado da seguinte forma:

- o Capítulo 2 apresenta uma revisão sobre os conceitos de certificação digital para documentos eletrônicos;
- o Capítulo 3 aborda a dificuldade para validar documentos eletrônico assinados e descreve soluções presentes na literatura para simplificar o uso de certificação digital;
- o Capítulo 4 apresenta os conceitos da Infraestrutura de Chaves Públicas Otimizadora e dos Certificados Otimizados;
- o Capítulo 5 descreve como foi construído um protótipo para testar a certificação digital otimizada;
- o Capítulo 6 apresenta uma análise sobre o Certificado Otimizado, lançando mão dos resultados obtidos nos testes sobre o protótipo, simulações e estimativas de esforço computacional;
- o Capítulo 7 finaliza este trabalho através das considerações finais e dos trabalhos futuros.

2 CERTIFICAÇÃO DIGITAL

2.1 INTRODUÇÃO

No mundo físico dispõe-se de mecanismos e procedimentos de segurança para proteger os usuários contra fraudes. Por exemplo, assinaturas de próprio punho, selos e lacres auxiliam-nos na verificação da autenticidade e integridade de documentos em papel. Por outro lado, tem-se agora um ambiente virtual de informações em que tais dispositivos tangíveis de segurança não são aplicáveis. Como solução surge a certificação digital.

Através da certificação digital os usuários de um ambiente virtual podem criar assinaturas digitais sobre um documento eletrônico – este último aqui definido como uma sequência de bits que codifica uma informação qualquer. Por exemplo, textos, imagens, sons ou até mesmo dados randômicos criados por um gerador de números aleatórios. Adicionalmente, a certificação digital proporciona suporte ao uso de identidades (certificados) digitais, artefatos úteis para identificar virtualmente um usuário bem como verificar as assinaturas digitais por ele criadas.

As seções a seguir têm o objetivo de fornecer embasamento teórico sobre certificação digital de documentos eletrônicos. Esses conceitos auxiliarão o leitor a compreender as dificuldades do uso de assinaturas digitais sobre documentos eletrônicos (Capítulo 3) como ainda a proposta de certificação otimizada (Capítulo 4).

O restante do capítulo é organizado da seguinte forma. As seções 2.2 e 2.3 apresentam, respectivamente, funções de resumo criptográfico e de criptografia de chave pública: conceitos envolvidos na criação e verificação de assinaturas digitais (Seção 2.4). A Seção 2.5 apresenta Infraestrutura de Chaves Públicas e o certificado digital X.509, cujos mecanismos de revogação são descritos nas seções 2.6 e 2.7. Por fim, a Seção 2.8 conclui este capítulo.

2.2 FUNÇÃO DE RESUMO CRIPTOGRÁFICO

Uma função de resumo criptográfico é uma função matemática F que mapeia um conjunto A, cujos elementos têm tamanho arbitrário, em um conjunto B, cujos elementos têm tamanho fixo. Em outras palavras, tem-se $F : A \longmapsto B$ tal que $A = \{x | x \in (0,1)^*\}$ e $B = \{y | y \in (0,1)^* \wedge |y| = n\}$, sendo $*$ o fechamento transitivo, $|w|$ o tamanho da sentença w e n um número natural. Por exemplo, a função SHA-1 [28] mapeia uma entrada de tamanho inferior a 2^{64} bits para uma saída de 128 bits (i.e. $n = 128$).

Adicionalmente, uma função de resumo criptográfico pode ser con-

siderada de *sentido único*. Neste caso, ela deve apresentar as seguintes propriedades [29]:

Resistência a colisão : é computacionalmente inviável obter $x \in A$ e $x' \in A$, tal que $x \neq x' \wedge F(x) = F(x')$;

Resistência a primeira pré-imagem : é computacionalmente inviável calcular $x = F^{-1}(y)$, tal que $x \in A$ e $y \in B \wedge y = F(x)$;

Resistência a segunda pré-imagem : é computacionalmente inviável obter $x' \in A$, dado $y = F(x)$, tal que $x \in A \wedge y \in B \wedge F(x) = F(x') = y$.

Devido a estas características, funções de resumo criptográfico podem ser utilizadas para representar uma informação de maneira compacta e anônima. Por exemplo, em um sistema de autenticação no qual o usuário prova a posse da senha correta submetendo o resumo criptográfico dela, sem a revelar. Ainda, tais funções são utilizadas para verificação de integridade. Por exemplo, uma mensagem pode ser enviada pela rede juntamente com seu resumo criptográfico. Ao recebê-los, o usuário recalcula o resumo criptográfico da mensagem e o compara com aquele recebido. Caso ambos coincidam, considera-se a mensagem íntegra.

Entre os algoritmos de resumo criptográfico mais difundidos podem-se citar SHA-1 e SHA-2 [30] e RIPEMD [31].

É importante ressaltar que o avanço de técnicas de criptoanálise ao longo dos anos tem sido capaz de comprometer as propriedades dos algoritmos de resumo criptográfico de sentido único, os quais passam então a ser considerados inseguros. Por exemplo, Wang et al. [32] e Yajima et al. [33] descrevem, respectivamente, ataques de colisão sobre os algorítimos MD4 e SHA-1, enquanto os trabalhos [34, 35] apresentam o comprometimento da resistência a primeira pré-imagem do algoritmo MD5. Todavia, a partir do momento em que a resistência a segunda pré-imagem é vencida, é possível se forjar a autenticidade de assinaturas digitais, as quais são apresentadas a seguir.

Por fim, vale lembrar que ainda não existem ataques de segunda pré-imagem ao SHA-1, porém seu uso é recomendado até o final de 2010 [36], quando então se sugerem utilizar algoritmos da família SHA-2. Esta, por sua vez, deverá ser substituída no futuro pelo SHA-3, para qual já há esforços de desenvolvimento [37].

2.3 CRIPTOGRAFIA DE CHAVE PÚBLICA

A criptografia de chave pública foi proposta por Diffie e Hellman [5] e é baseada em uma função de criptografia F e um par de chaves (D, E). Toda operação de cifragem com F, cujas entradas são x e uma chave do par, pode ser decifrada pela mesma função F, porém operando com a outra chave do par. Em outras palavras, $F(D, F(E, x)) =$

$F(E, F(D, x)) = x$, tal que $|x| = |D| = |E|$, sendo $|x|$ o tamanho de x.

A geração do par de chaves (D, E) é baseado em problemas matemáticos intratáveis (e.g. fatoração de números compostos grandes), fato que torna computacionalmente inviável a derivação de uma chave a partir da outra do mesmo par. Dessa maneira, tal esquema de criptografia permite a divulgação de uma das chaves, a qual é denominada chave pública. A outra chave, que deve ser mantida sob sigilo, recebe o nome de chave privada.

Entre os algoritmos de criptografia de chave pública mais difundidos podem-se citar RSA [38] e curvas elípticas [39].

Uma das motivações para a concepção da criptografia de chave pública foi simplificar a gerência de chaves, desafio presente na criptografia simétrica. Nesta, a chave simétrica é utilizada para cifrar e decifrar uma informação, portanto o usuário precisa estabelecer uma chave distinta para cada participante. Por outro lado, na abordagem de chave pública o usuário utiliza um par de chaves para todos os participantes.

Finalmente, a abordagem de chave pública é largamente utilizada para prover autenticação. Tal mecanismo de segurança computacional pode ser obtido através da criação e verificação de assinaturas digitais, as quais são apresentadas a seguir.

2.4 ASSINATURA DIGITAL

A assinatura digital é uma informação através da qual um signatário atesta sua ciência sobre a veracidade do documento eletrônico assinado. O processo de assinatura consiste em cifrar com a chave privada o resumo criptográfico calculado sobre um documento eletrônico, como ilustra a Figura 2.1. Por outro lado, terceiros verificam uma assinatura digital decifrando-a e a comparando com o resumo criptográfico calculado sobre o documento eletrônico, como ilustra a Figura 2.2.

A assinatura digital garante integridade e autenticidade simultaneamente. A primeira é assegurada devido à assinatura digital embarcar e proteger o resumo criptográfico do documento eletrônico, o qual permite a posterior verificação de integridade. A segunda é garantida pelo fato de que apenas o detentor da chave privada é capaz de gerar a assinatura digital sobre o documento eletrônico, o que comprova a autenticidade deste.

Todavia, a comprovação de autenticidade da assinatura digital pode ser comprometida caso a chave pública utilizada por terceiros na verificação não pertença de fato ao signatário. Desta maneira, houve a necessidade de se criarem soluções que atrelassem a identidade do signatário a sua chave pública. Entre as alternativas que se destacaram estão os certificados digitais, os quais são apresentados a seguir.

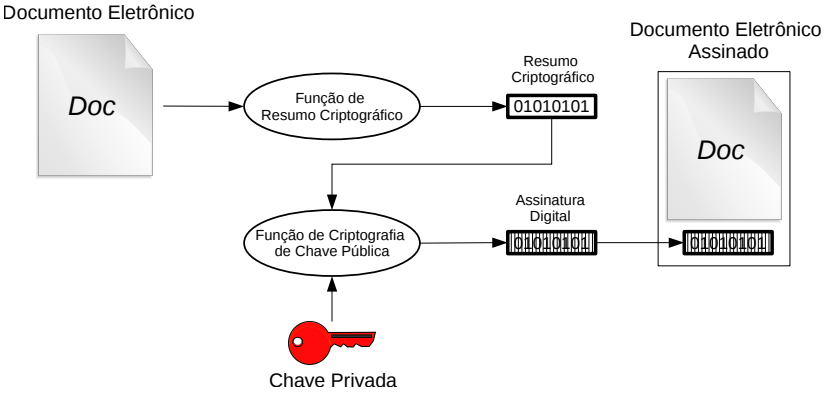

Figura 2.1: Criação de assinatura digital.

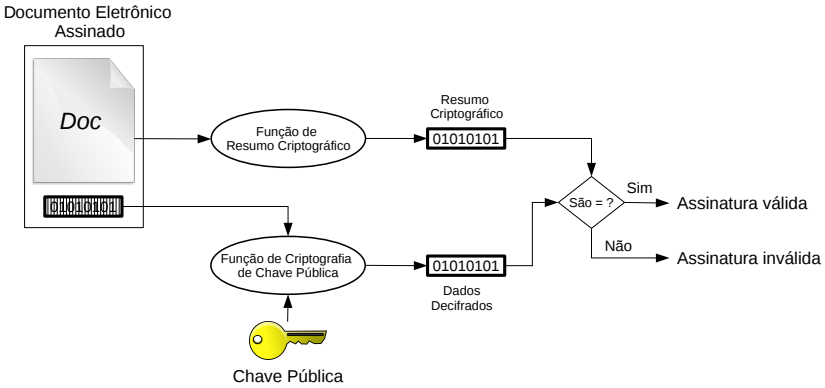

Figura 2.2: Verificação de assinatura digital.

2.5 INFRAESTRUTURA DE CHAVES PÚBLICAS

Além de apresentar o conceito de criptografia de chave pública, Diffie e Hellmann [5] descrevem o papel do Arquivo Público. Este é uma entidade central de consulta de chaves públicas pertencentes a usuários do domínio do Arquivo Público. Ainda, toda resposta de consulta é assinada pelo Arquivo Público, de modo a prover segurança à comunicação.

A Figura 2.3 ilustra o Arquivo Público e seu papel centralizador de custódia de chaves públicas dos usuários. Para obter uma chave pública arbitrária, um usuários consulta o Arquivo Público, submetendo informações sobre o titular da chave pública. Por exemplo, o nome. Essa etapa é destacada na Figura 2.3 por *1*. Em seguida, o Arquivo Público localiza a chave pública solicitada (*2*), com a qual monta a resposta à consulta do usuário. Depois, a resposta é assinada com a chave privada do Arquivo Público (*3*), garantindo autenticidade e integridade. Por fim, o

Arquivo Público envia ao usuário a resposta assinada, que contém a chave publica solicitada (*4*).

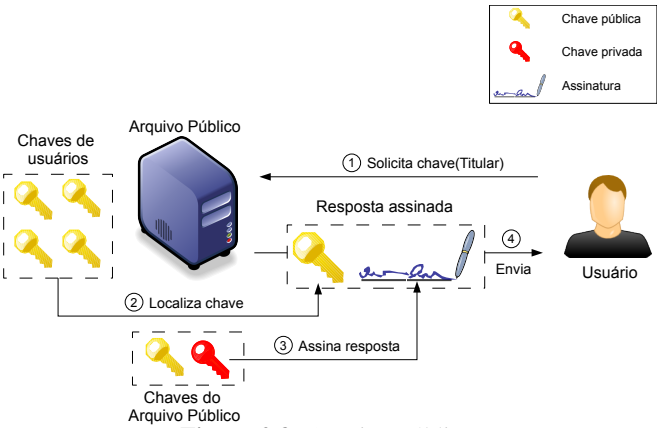

Figura 2.3: Arquivo Público.

Entretanto, esta configuração centralizada, em que se assinam todas as respostas do Arquivo Público, representa um gargalo de eficiência, bem como um ponto central de falha. Ou seja, uma vez indisponível o Arquivo Público nenhuma chave pública poderia ser obtida. Visando solucionar este problema, Kohnfelder [6] propôs o conceito de certificado digital: uma estrutura assinada por uma Autoridade Certificadora (AC) com o objetivo de certificar a relação entre uma chave pública e a identidade de seu titular. Assim, por ser um objeto digital assinado, o certificado pode ser replicado, eliminando-se a necessidade de um Arquivo Público. Desta maneira, o certificado pode ser largamente utilizado para a distribuição de chaves públicas bem como para a verificação de assinaturas digitais. A Figura 2.4 ilustra novamente a verificação de assinatura digital, todavia obtendo-se a chave pública a partir do certificado digital.

Logo após serem propostos, os certificados digitais passaram a ser utilizados em diretórios globais e hierárquicos X.500 [40] – administrados por grandes empresas de telecomunicação. Em cada nível da hierarquia do diretório havia uma AC cuja finalidade era emitir certificados para: a) usuários autorizados acessarem informações daquele nível; b) ACs de níveis inferiores. A identidade de ACs e usuários eram apresentadas nos certificados através de *Relative Distinguished Name*s (RDN) como ilustra a Figura 2.5.

Com base no emprego de certificados nos diretórios X.500 foi proposto o padrão X.509v1 [41]. Anos depois foram lançadas as versões X.509v2 [42] e, mais recentemente, X.509v3 [43]. Os campos do certificado X.509v3 são apresentados na Tabela 2.1.

Segundo Housley e Polk [44], usuários de certificados digitais em um cenário ideal seriam capazes de determinar imediatamente quando

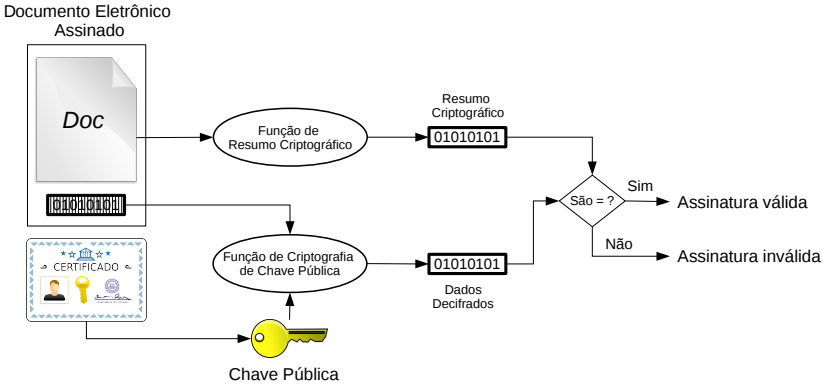

Figura 2.4: Verificação de assinatura digital a partir de um certificado digital.

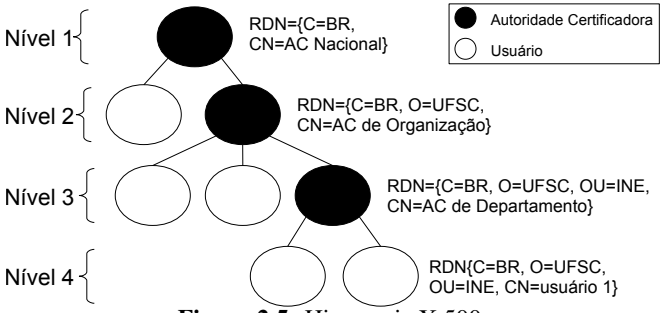

Figura 2.5: Hierarquia X.500.

uma informação contida em um certificado se tornasse inválida. Todavia, sabe-se que isso não é possível na prática, pois é inviável localizar e destruir todas as cópias de um certificado cujas informações tornaram-se inválidas, dado que ele pode ter sido replicado e distribuído indefinidamente. Desta maneira, adota-se a solução de revogar um certificado.

O processo de revogação consiste em publicar que determinado certificado tornou-se inválido. Tal procedimento é realizado pelo emissor do certificado, o qual faz uso de dispositivos de revogação. Destes, os mais difundidos são as Listas de Certificados Revogados e *Online Certificate Status Protocol*. Ambos são descritos nas seções a seguir.

2.6 LISTA DE CERTIFICADOS REVOGADOS

A Lista de Certificados Revogados (LCR), especificada em [45], também é um objeto digital assinado que pode ser replicado e distribuído. Através da emissão de uma LCR, uma AC divulga quais dos certificados por ela emitidos se tornaram inválidos, e, portanto, devem ser considerados como revogados. Alternativamente, uma AC pode delegar a emissão

Tabela 2.1: Campos do certificado X.509v3

Campo	Descrição	Exemplo
Version	Versão do certificado	3
Serial Number	Número de série	100
Signature Algorithm	Identificação do algoritmo de assinatura	*ecdsa-with-SHA1*
Issuer	Identificação emissor do certificado	*C=BR, ST=SC, L=Florianopolis, O=UFSC, OU=LabSEC, CN=AC Final*
Validity	Define o fim e o início do prazo de validade do certificado	*notBefore:20100327230800Z notAfter:20110327230800Z*
Subject	Identificação do titular da chave pública	*C=BR, ST=SC, L=Florianopolis, O=UFSC, OU=LabSEC, CN=Martin*
Subject Public Key Info	Dados sobre a chave pública do titular	*id-ecPublicKey*, *pub:04:a2:45:03:36:16:83*, *ASN1 OID: secp224r1*
X.509v3 Extensions	Extensões X.509v3	*Basic Constraints*
Signature	Assinatura do emissor do certificado	*ecdsa-with-SHA1*, *30:3d:02:1d:00:c5:a5:1b*

de LCR a outra entidade.

De maneira similar ao certificado, a LCR contém a identificação e assinatura digital de seu emissor, um número de série e um prazo de validade. A LCR apresenta certificados revogados na forma de uma lista, em que cada entrada contém a data da revogação, o número de série do certificado revogado e um campo opcional. Neste último pode-se, por exemplo, informar o motivo da revogação.

Dentre os motivos de revogação possíveis, destaca-se aquele que alerta para o comprometimento da chave privada relacionada ao certificado digital. Deve-se atentar para tal fato, uma vez que não se pode comprovar a autenticidade de assinaturas digitais criadas com uma chave privada comprometida. A Tabela 2.2 apresenta os motivos mais utilizados entre aqueles previstos em [45].

De modo a evitar o crescimento indefinido da LCR, esta deve conter apenas certificados revogados que ainda não expiraram. Entretanto, algumas ACs desrespeitam tal regra, mantendo nas LCRs todos os certificados revogados, independente da expiração. Se por um lado essa prática permite às ACs manterem um histórico de revogações útil a pesquisas retroativas sobre revogação, por outro impacta diretamente nos custos computacionais exigidos para manipular uma LCR.

Embora as LCRs sejam o meio de publicação de informação (situação) de revogação mais utilizado, elas apresentam limitações: a

Tabela 2.2: Motivos de revogação para certificados digitais.

Motivo	Descrição
unspecified	Motivo indefinido.
keyCompromise	Comprometimento de chave privada.
affiliationChanged	Modificada a identificação do titular ou outra informação contida no certificado digital, sem, entretanto, haver comprometimento da chave privada.
superseded	O certificado digital foi substituído por outro, sem, entretanto, haver comprometimento da chave privada.
cessationOfOperation	O certificado digital não é mais necessário à finalidade para que foi emitido.

presença de dados desnecessários ao verificador de certificado bem como a latência das informações. Em outras palavras, não é possível consultar a situação de revogação de um certificado particular sem a obtenção de toda LCR, a qual inclui informações de outros certificados. Além disso, o período para atualização da LCR pode ser longo, expondo o verificador ao risco de obter uma situação de revogação desatualizada. Como solução a alguns desses problemas há o *Online Certificate Status Protocol*, especificado em [46] e descrito a seguir.

2.7 *ONLINE CERTIFICATE STATUS PROTOCOL*

O *Online Certificate Status Protocol* (OCSP) é um serviço *online* de ICP através do qual pode-se consultar a situação de revogação de um ou mais certificados emitidos por uma AC particular. O tamanho do resultado de uma consulta é normalmente inferior ao de uma LCR, uma vez que o conteúdo do primeiro refere-se à situação de revogação de um conjunto arbitrário de certificados, enquanto a LCR contém informações sobre todos os certificados revogados e não expirados.

Outra vantagem do OCSP sobre a LCR é a latência das informações. Dependendo da implementação, o OCSP pode permitir a imediata publicação de mudanças da situação de revogação, enquanto no outro mecanismo as atualizações apenas se tornam disponíveis na publicação da LCR. Adicionalmente, o OCSP permitiria cobrar dos usuário as consultas a informações de revogação, ideia sugerida Peter Gutmann [17].

O serviço de OCSP pode ser disponibilizado diretamente por uma AC, a qual informa a situação de revogação dos certificados por ela emitidos. Todavia, de modo a preservar a integridade de uma AC, é comum que ela seja mantida isolada, ou seja, *offline*. Desta maneira, uma AC pode delegar o serviço OCSP a uma entidade *online*. Para tal, a AC emite um certificado digital à entidade. Esse certificado deve encapsular uma extensão X.509v3 que sinaliza a delegação do serviço OCSP.

Por fim, vale lembrar que as respostas do serviço OCSP são as-

sinadas pela AC *online* ou por uma entidade delegada. Portanto, tanto as respostas assinadas quanto o certificado da entidade signatária devem ser verificados pelos usuários de modo a prevenir fraudes. Todavia, este requisito pode ser simplificado no caso do serviço OCSP ser delegado, excluindo-se a verificação de certificado. Entretanto, ao adotar tal medida deve-se estar ciente dos riscos assumidos, uma vez que se trata de serviços *online* e que, portanto, estão expostos a ataques.

2.8 CONCLUSÃO

Este capítulo apresentou os conceitos necessários para compreender a certificação digital de documentos eletrônicos. Inicialmente, descreveram-se o resumo criptográfico e a criptografia de chave pública, que combinados permitem a criação e verificação de assinaturas digitais. Estas, por sua vez, garantem autenticidade e integridade a documentos eletrônicos. Em seguida, abordaram-se os certificados digitais, artefatos assinados que sintetizam a relação entre a identidade de um usuário e sua respectiva chave pública. Adiante, explicou-se a Infraestrutura de Chaves Públicas (ICP), alicerce de suporte para a certificação digital. Por fim, apresentaram-se os mecanismos mais comuns de revogação de certificados digitais, úteis para alertar usuários de uma ICP sobre certificados que se tornaram inválidos.

3 VALIDAÇÃO DE DOCUMENTOS ELETRÔNICOS ASSINADOS

3.1 INTRODUÇÃO

O capítulo anterior apresentou os conceitos da certificação digital, tecnologia que permite assegurar autenticidade e integridade a documentos eletrônicos. Agora, este capítulo dedica-se a descrever a validação de documentos eletrônicos assinados, processo que envolve verificar a assinatura digital bem como o certificado do signatário.

Faz-se, ainda, uma análise da dificuldade para validar documentos eletrônicos assinados considerando-se a manutenção da autenticidade da assinatura digital – processo necessário para estender o prazo de validade da assinatura digital através da inclusão de novas evidências. Por exemplo, carimbos do tempo. Em seguida, frente aos desafios discutidos, apresentam-se soluções disponíveis na literatura, dentre as quais algumas são utilizadas como base para a certificação otimizada, descrita no capítulo a seguir.

O restante do capítulo é organizado da seguinte forma. A Seção 3.2 descreve a validação de documentos assinados. A Seção 3.3 aborda a inclusão de carimbos do tempo para estender a validade de assinaturas digitais. A Seção 3.4 apresenta os padrões de formato de assinatura digital. As seções 3.5 e 3.6 expõem desafios e respectivas soluções presentes na literatura para o uso de documentos eletrônicos assinados. Por fim, a Seção 3.7 conclui este capítulo.

3.2 PROCESSO DE VALIDAÇÃO

Para validar um documento eletrônico assinado é necessário verificar: a) a assinatura digital; e b) o certificado digital do signatário. A primeira validação consiste em operações criptográficas com a chave pública do signatário, garantindo a integridade e a autenticidade da assinatura - o que equivale a dizer, respectivamente, que o documento não sofreu alterações posteriores à sua assinatura e que esta foi produzida de fato pela chave privada relacionada à chave pública do signatário. A segunda validação é efetuada a fim de garantir a irretratabilidade da assinatura, ou seja, que o par chaves do signatário era válido no momento da criação da assinatura, assegurando-se, por exemplo, que a chave privada não tenha sido previamente roubada e, então, utilizada por terceiros. Neste caso utiliza-se o algoritmo *Certificate Path Processing* [11], que consiste em construir e validar o caminho de certificação do signatário.

Na construção do caminho de certificação se deve encontrar pelo menos uma sequência de certificados que ligue a entidade final (e.g. o

signatário de um documento eletrônico) a uma âncora de confiança auto-assinada. A sequência não inclui o certificado de âncora de confiança. De forma a ilustrar tal conceito, a Figura 3.1 apresenta uma ICP de 4 níveis. No topo da ICP está a âncora confiança (*AC Raiz*), entidade que emite seu próprio certificado, bem como o da AC_1. Esta emite o certificado da AC_2, que, por sua vez, emite o certificado da entidade final (*Signatário*). Neste caso, o caminho de certificação da entidade final é composto pelos certificados presentes nos níveis 2 a 4.

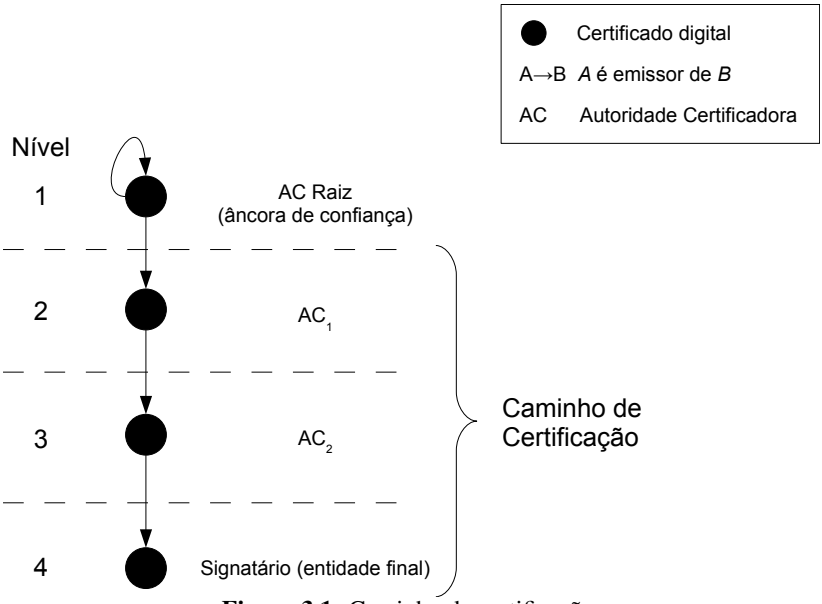

Figura 3.1: Caminho de certificação.

Para validar o caminho de certificação deve-se verificar os certificados de cada sequência de acordo com:

- a integridade e a autenticidade da assinatura de cada certificado digital devem ser verificadas através da chave pública de seu emissor;
- o período de validade de cada certificado digital deve incluir o momento de criação da assinatura;
- um certificado digital não pode ter sido revogado antes da criação da assinatura;
- os nomes de titular ou emissor seguem as restrições de nomes, caso existam;
- o certificado digital obedece a todas as políticas de certificação que sobre ele incidem dentro de sua respectiva ICP.

É importante citar a importância da referência temporal utilizada na verificação do caminho de certificação. Isto se deve ao fato de que a validade de um certificado pode mudar ao longo do tempo. A Figura 3.2 ilustra como a validade do caminho de certificação apresentado na Figura 3.1 depende da referência temporal.

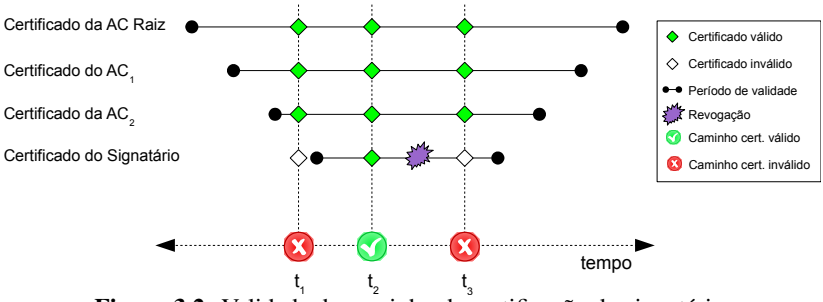

Figura 3.2: Validade do caminho de certificação do signatário.

Na Figura 3.2 observa-se que o caminho de certificação é inválido em t_1, uma vez que este instante está fora do prazo de validade do certificado do signatário. Em t_2 o caminho de certificação é válido, dado que todos os certificados estão válidos no mesmo instante. Por fim, em t_3 o caminho de certificação é inválido, dado que o certificado do signatário foi revogado antes de t_3.

Quando não se sabe o momento em que uma assinatura digital foi criada, é recomendável que a referência temporal seja o instante em que se efetua a verificação do caminho de certificação do signatário. A justificativa para tal está na consulta à última situação de revogação dos certificados, evitando assim desconsiderar uma revogação recente. Todavia, é possível que o caminho de certificação fosse válido no momento da criação da assinatura, deixando de ser válido posteriormente devido à revogação ou até a expiração de algum certificado no caminho de certificação signatário. Neste caso, a assinatura seria considerada inválida, a menos que se conheça um momento passado em que a assinatura já existia e ainda era válida. Tal informação temporal sobre a assinatura pode ser disponibilizada de maneira segura para verificadores através de carimbos do tempo, descritos a seguir.

3.3 CARIMBO DO TEMPO

O carimbo do tempo [12] é um documento eletrônico assinado cujo conteúdo informa que um dado arbitrário já existia na data de emissão do carimbo do tempo. Este é emitido por uma Autoridade de Carimbo do Tempo (ACT), a qual possui um relógio sincronizado com uma fonte de tempo confiável. Portanto, carimbos do tempo foram concebidos para serem usados como referências temporais confiáveis no processo de

validação de documentos assinados.

A Figura 3.3 ilustra a presença de um carimbo do tempo na validação de uma assinatura sobre um documento eletrônico. Inicialmente, em t_{sig}, o signatário, de posse de um certificado digital válido, assina um documento eletrônico. Em seguida, em t_{ct} um carimbo do tempo é emitido para a assinatura digital sobre o documento eletrônico. Logo, o certificado do signatário é revogado após t_{ct}.

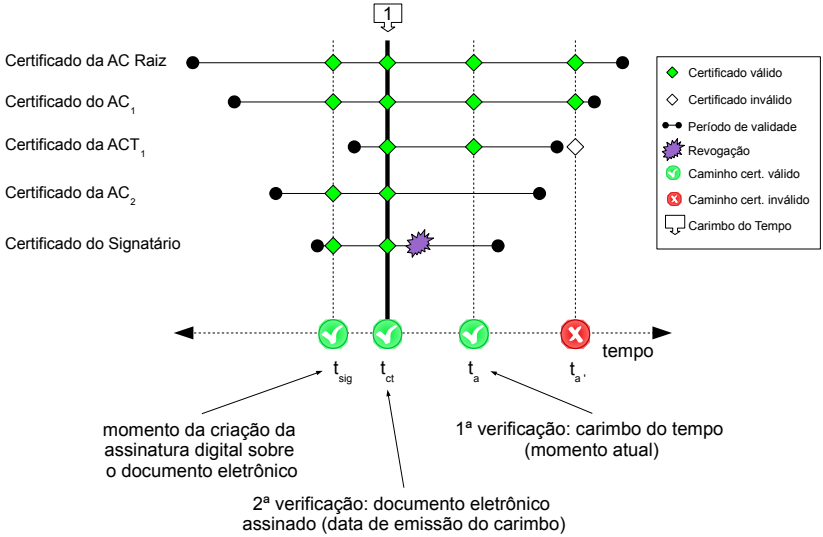

Figura 3.3: Validade dos caminhos de certificação da ACT e do signatário.

Para validar a assinatura digital o verificador verifica, primeiramente, a validade do carimbo do tempo no momento atual (t_a). Ou seja, verificam-se a assinatura digital sobre o carimbo do tempo e o caminho de certificação da ACT_1 no instante t_a. Caso o carimbo do tempo seja válido, o verificador verifica a assinatura digital sobre o documento eletrônico no instante t_{ct} ao invés de t_{sig}, dado que há evidências (i.e. o carimbo do tempo 1) de que a assinatura digital já existia naquele momento. Nota-se que, embora o certificado do signatário não seja mais válido em t_a, pode-se verificar com sucesso a assinatura digital sobre o documento eletrônico. Isto é possível pois o carimbo do tempo informa que a assinatura digital já existia antes de o certificado do signatário ser revogado.

Mais adiante no tempo, em $t_{a'}$, o carimbo do tempo não é válido, pois o certificado da ACT_1 expirou. Como consequência, perde-se a evidência confiável sobre o momento (t_{ct}) em que já existia a assinatura digital. Portanto, esta não pode ser mais validada.

Todavia, similarmente a um documento eletrônico, a validade de um carimbo do tempo pode ser estendida através de outro carimbo do

tempo. Este irá garantir que a assinatura digital sobre aquele já existia antes de o caminho de certificação do signatário (i.e. ACT_1) tornar-se inválido, como ilustra a Figura 3.4.

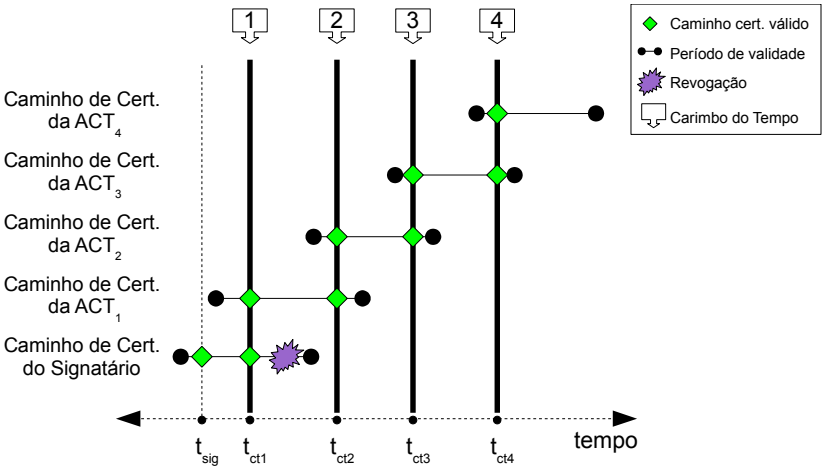

Figura 3.4: Encadeamento de carimbos do tempo.

Na Figura 3.4 vê-se que uma assinatura digital sobre um documento eletrônico é criada em t_{sig} quando o caminho de certificação do signatário está válido. Em seguida, em t_{ct1} emite-se um carimbo do tempo para assinatura digital. Nesse momento os caminhos de certificação do signatário e da ACT_1 devem ser válidos. Mais a frente, para estender a validade do carimbo do tempo 1, adiciona-se, em t_{ct2}, o carimbo do tempo 2 para a assinatura sobre o carimbo do tempo 1. Novamente, os caminhos de certificação da ACT_1 e ACT_2 devem estar válidos em t_{ct2}. Este processo repete-se em t_{ct3}, t_{ct4} e assim por diante, sempre antes de terminar a validade do caminho de certificação da ACT que emitiu o carimbo do tempo vigente.

Além de serem úteis para informar que uma assinatura digital já existia antes do caminho de certificação do signatário se tornar inválido, os carimbos do tempo são utilizados também para contingenciar o envelhecimento dos algoritmos criptográficos. Neste caso, o carimbo do tempo de arquivamento permite a um verificador saber se um documento eletrônico foi assinado antes de os algoritmos criptográficos utilizados terem se tornado inseguros.

Por fim, a adição contínua de carimbos do tempo é uma das técnicas da manutenção da autenticidade de documentos eletrônicos assinados. Todavia, de forma a garantir a interoperabilidade dos documentos eletrônicos e das evidências a eles anexadas durante a manutenção de autenticidade, utilizam-se padrões de formatos de assinatura digital. Estes são abordados a seguir.

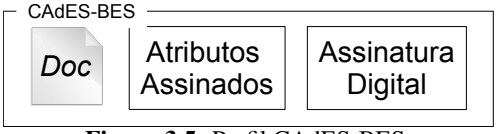

Figura 3.5: Perfil CAdES-BES.

3.4 PADRÕES DE FORMATOS DE ASSINATURA DIGITAL

Os padrões de formatos de assinatura digital tem como objetivo garantir a interoperabilidade entre sistemas computacionais que participam de transações seguras. É função de um padrão definir como serão estruturadas a assinatura e dados a ela acrescidos, como ainda a maneira em que tais informações devem ser processadas.

Os padrões mais comuns podem ser divididos em dois grupos de acordo com a linguagem de descrição de dados utilizada: *Abstract Notation One* (ASN.1) [47] e *Extensible Markup Language* (XML) [48]. Com base na primeira, têm-se o *Public Key Cryptography Standards #7* (PKCS#7) [49] e seu sucessor, o *Cryptographic Message Syntax* (CMS) [50]. Entre aqueles baseados na segunda, destaca-se o *XML-Signature Syntax and Processing* (XMLdSig) [51].

No entanto, os padrões citados não contemplam a manutenção da autenticidade de assinaturas digitais. Preocupada com isso, a União Européia, através do *European Telecommunications Standards Institute* (ETSI), passou a promover perfis avançados de assinatura digital, que diferem de acordo com os tipos de evidências de autenticidade utilizados e o tempo de validade estipulado para a assinatura. Estes perfis são implementados em documentos PDF (*PDF Advanced Electronic Signatures* – PAdES [52, 53, 54]), em XML (*XML Advanced Electronic Signatures* – XAdES [55]) e em ASN.1 (*CMS Advanced Electronic Signatures* – CAdES [56]), o qual é apresentado a seguir.

O perfil básico, denominado CAdES-BES é ilustrado na Figura 3.5 e apresenta uma estrutura que encapsula: a) um documento eletrônico, cuja presença no formato é opcional; b) um conjunto de atributos assinados e c) uma assinatura digital calculada sobre os itens a) e b).

Se por um lado o uso do CAdES-BES requer o mínimo de recursos de armazenamento, por outro a verificação da assinatura exige do verificador recursos adicionais de processamento e de comunicação. Isso porque o verificador precisa descobrir quais são os certificados digitais necessários para a construção do caminho de certificação do signatário. Este processo consiste em acessar diferentes repositórios e buscar relações (e.g. encadeamento de nomes [57]) entre os certificados disponíveis até que um caminho de certificação seja montado. Em seguida, o verificador precisa obter uma cópia dos certificados e respectivas informações de revogação para validar o caminho de certificação construído.

Percebe-se, ainda, que o CAdES-BES não prevê carimbos do

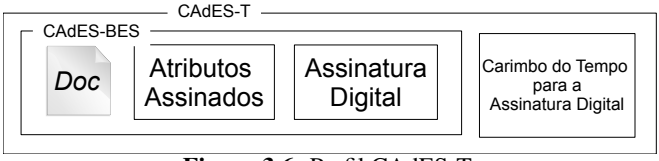

Figura 3.6: Perfil CAdES-T.

tempo. Portanto, recomenda-se usar esse perfil para situações em que o prazo de validade da assinatura é inferior ao do certificado do signatário. Por exemplo, um sistema computacional cuja autenticação de usuários é feita através da troca de mensagens assinadas.

O perfil CAdES-T (Figura 3.6) tem como objetivo prover uma referência de tempo para a assinatura. Assim, a assinatura digital pode ser verificada mesmo após o caminho de certificação do signatário tornar-se inválido, como descrito na Seção 3.3. Ainda, de maneira semelhante ao CAdES-BES, fica a cargo do verificador a descoberta e localização de certificados e informações de revogação (LCRs ou OCSP) referentes aos caminhos de certificação do signatário e da ACT que emitiu o carimbo do tempo.

O perfil CAdES-C (Figura 3.7) prevê referências completas aos certificados e LCRs/OCSPs do signatário, eliminando o esforço do verificador em descobrir tais evidências de autenticidade. Não obstante, ainda cabe ao verificador descobrir os certificados e informações de revogação atuais da ACT que emitiu o carimbo do tempo sobre a assinatura. Também é função do verificador localizar todos os certificados e LCRs/OCSPs referentes aos caminhos de certificação do signatário e da ACT, como no ocorre no CAdES-T.

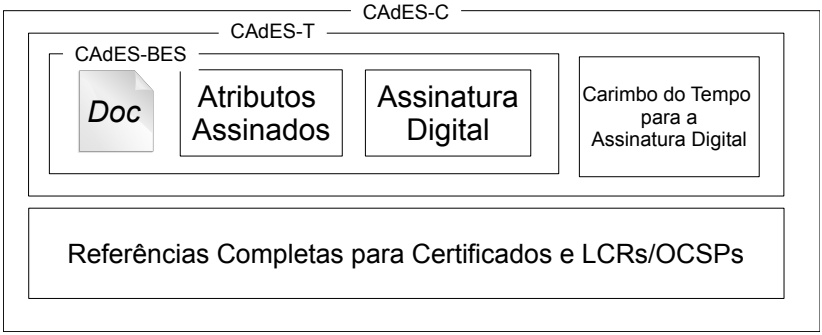

Figura 3.7: Perfil CAdES-C.

O perfil CAdES-X Long (Figura 3.8) permite que os certificados e LCRs/OCSPs do caminho de certificação do signatário sejam embarcados no formato. O perfil prevê um carimbo do tempo adicional (sobre o CAdES-C ou apenas sobre as referências), cujo objetivo é prover uma

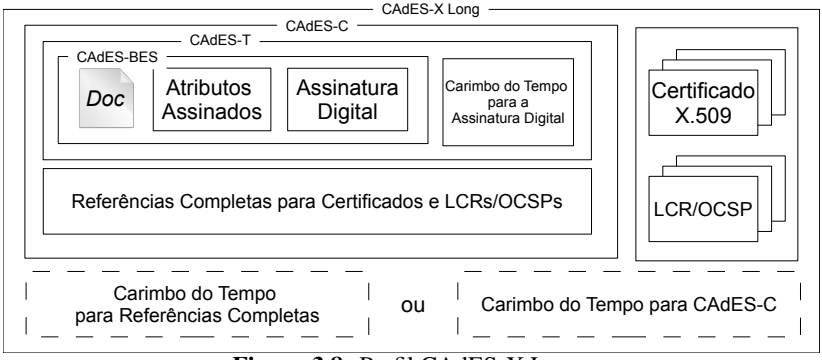

Figura 3.8: Perfil CAdES-X Long.

referência temporal sobre todo o caminho de certificação do signatário. Desta maneira, o comprometimento de uma AC intermediária no caminho de certificação do signatário não invalidará a assinatura, o que pode ocorrer no CAdES-T e -C. Por fim, vale lembrar que cabe ao verificador descobrir e localizar todas as evidências de autenticidade para os dois carimbos do tempo presentes no formato.

O perfil CAdES-A (Figura 3.9) é recomendado para arquivamento de documentos eletrônicos assinados. Ele prevê um ou mais carimbos do tempo de arquivamento, os quais atestam a existência de todos os elementos do formato. Desta maneira, devem ser incluídos obrigatoriamente o documento eletrônico com todos os certificados e LCRs dos caminhos de certificação do signatário e dos carimbos do tempo anteriores ao de arquivamento. Todavia, fica a cargo do verificador descobrir e localizar os certificados e LCRs atuais do caminho de certificação da ACT emissora do último carimbo do tempo de arquivamento.

3.5 DESAFIOS PARA O USO A LONGO PRAZO DE DOCUMENTOS ASSINADOS

Ao analisarmos os diversos requisitos para criação e verificação de documentos eletrônicos assinados percebemos o esforço computacional decorrente da complexidade da Infraestrutura de Chaves Públicas. O principal exemplo refere-se à validação da assinatura digital sobre um documento eletrônico, o qual demanda a verificação de autenticidade e integridade da assinatura bem como de sua irretratabilidade. Esta última é avaliada através da construção e verificação do caminho de certificação do signatário.

A construção do caminho de certificação exige a descoberta e a localização de artefatos (e.g. certificados e LCRs). Ou seja, identificar os dados de validação e obter uma cópia destes, respectivamente. Tais passos dependem da estrutura da assinatura digital, a qual pode embar-

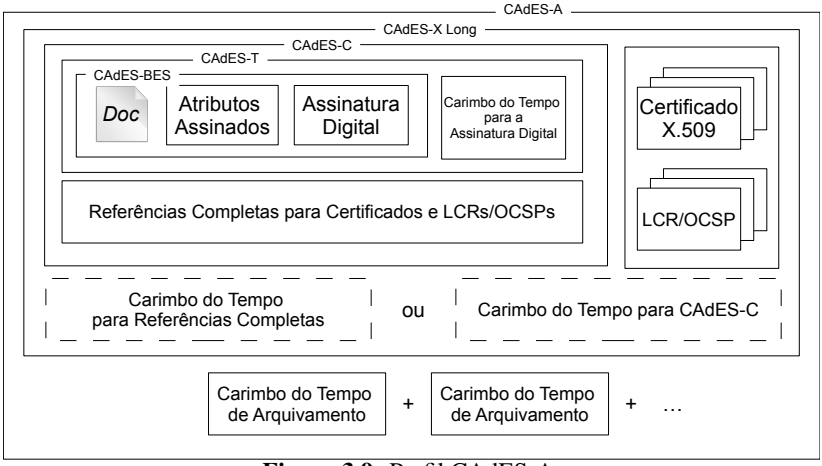

Figura 3.9: Perfil CAdES-A.

car os artefatos. Caso embarque, remove-se do verificador o esforço de comunicação para consultar repositórios externos. Porém, em contrapartida, exige-se um maior esforço de armazenamento.

A verificação do caminho de certificação avalia a validade de cada certificado do caminho de certificação. Em tal processo destaca-se a verificação das assinaturas digitais sobre os certificados bem como sobre as informações de revogação. Portanto, há o esforço de processamento, o qual é proporcional ao tamanho do caminho de certificação [58].

Em documentos assinados mantidos por longo prazos a manutenção da autenticidade da assinatura causa o aumento linear da quantidade de artefatos. Assim, é evidente o aumento dos esforços de processamento e armazenamento. Embora o último possa ser atenuado, é recomendável incorporar os artefatos na assinatura digital, uma vez que eles podem não estar disponíveis no futuro em repositórios.

Por fim, é importante mencionar que há outro fator que pode contribuir na dificuldade de se usarem documentos eletrônicos assinados: os mecanismos de revogação de certificados. É o caso das LCRs, que são largamente difundidas e podem se tornar muito longas. Por exemplo, após 1 ano de operação, a ICP da Johnson&Johnson continha 30.000 certificados revogados [59]. Outro exemplo é a LCR emitida pela Autoridade Certificadora para a Secretaria da Receita Federal (ICP-Brasil) [60] a qual apresentava 9.263 certificados revogados. Como alternativa há OCSP, todavia suas respostas geralmente carecem de verificação de autenticidade e irretratabilidade, exigindo também a consulta a LCRs.

3.6 TRABALHOS RELACIONADOS

As dificuldades envolvidas no emprego de assinatura digital são tema de discussão há anos. Diversas soluções foram propostas, sendo as mais relevantes apresentadas a seguir.

Os certificados aninhados [14] têm o objetivo de diminuir o número de operações criptográficas para se verificar um caminho de certificação. A ideia consiste em emitir certificados para outros certificados, resultando em um caminho de certificação aninhado cuja validação é efetuada verificando-se a assinatura do primeiro certificado aninhado do caminho e, em seguida, comparando-se resumos criptográficos dos demais certificados, dispensando-se a verificação da assinatura destes.

Adicionalmente, há a possibilidade de se delegar a tarefa de validação do caminho de certificação para entidades denominadas verificadores. Exemplos de verificadores são OCSP [46], OCSP *Extensions* (OCSP-X) [61], *Simple Certificate Validation Protocol* (SCVP) [62], e *Data Validation and Certification Server Protocol* (DVCS) [63]. Tais soluções transferem o custo computacional da validação para um verificador, o qual exerce o papel semelhante a de um notário, atestando para terceiros a validade de um certificado.

Outros trabalhos concentram-se nos problemas de revogação na ICP. Há proposta de certificados de curta duração [15] cujo tempo de vida é tão reduzido – por exemplo, 1 dia – que a probabilidade de serem revogados é praticamente zero. Desta maneira, podem-se eliminar da ICP o serviço de revogação e as desvantagens decorrentes de seu uso. Este esquema de certificação é empregado, por exemplo, na *Infraestrutura Simples de Chaves Públicas* (SPKI) [23, 24].

Entretanto, os certificados de curta duração não são adequados para ACs e ACTs, cujo tempos de vida são geralmente longos. Ainda, na maioria dos cenários de certificação digital o uso de revogação é indispensável. Além disso, onde a revogação de certificados pode ocorrer, trabalhos como [64, 65] estimam que 10% de todos os certificados são revogados. Neste contexto destacam-se os seguintes trabalhos que focam nos problemas de baixa escalabilidade e alto custo das LCRs: *Delta CRL* [11], *CRL Distribution Points* [11], *Windowed CRL* [66], *Over-issued CRL* [67], *Blacklist CRL* [68], *Redirected Pointers* [69], *Certificate Revocation Trees* [70] e *Certificate Revocation Status* (CRS), também conhecido como Novomodo [16]. Para este se dedica a seção a seguir.

3.6.1 Método de Revogação Novomodo

No método Novodomo [16] uma AC publica a situação de revogação de cada certificado não expirado. Antes de emitir um certificado, a AC define o intervalo de tempo (l) entre duas publicações de situação de revogação consecutivas (e.g. $l = 1$ dia) e dois valores secretos aleatórios (X_0 e Y_0). Em seguida, a partir de uma função de resumo

criptográfico F, a AC gera os alvos de validade ($X_n = F^n(X_0)$) e de revogação ($Y_1 = F^1(Y_0)$), sendo n o total de publicações de situação de revogação ao longo do prazo de validade do certificado (e.g. $n = 365$) e $F^j(b) = F(F^{j-1}(F^{j-2}(...F^1(b)...)))$. No próximo passo, o certificado é emitido e X_n e Y_1 são publicados, podendo ser embarcados no próprio certificado.

Durante o prazo de validade do certificado a AC libera S_k, dado que corresponde à $k-$ésima situação de revogação do certificado, sendo $0 < k < n$. Se o certificado está revogado, então $S_k = Y_0$, senão ele é válido e $S_k = X_{n-k}$, valor denominado prova de validade. A Figura 3.10 ilustra este processo.

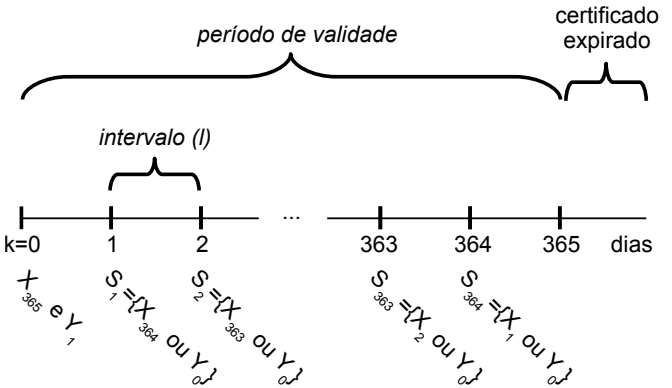

Figura 3.10: Publicação da situação de revogação de um certificado digital utilizando o método Novomodo.

Os verificadores do certificado obtém S_k de um repositório. Em seguida executam o Algoritmo 1 e determinam a validade do certificado.

O Novomodo destaca-se entre os demais sistemas de revogação devido ao baixo esforço computacional necessário para implementá-lo. Isto se deve às informações de revogação serem de tamanho fixo e reduzido, bem como facilmente geradas e verificadas através de funções de resumo criptográfico. Além disso, ganha-se em performance ao não se utilizarem assinaturas digitais para garantir a autenticidade de S_k. Isso porque a falsificação de $S_k = X_{n-k}$ a partir $S_{k-1} = X_{n-k+1}$ requer calcular $F^{-1}(X_{n-k+1})$, operação computacionalmente inviável.

Por fim, as características acima mencionadas fazem do método Novomodo uma atraente solução de revogação para ambientes com restrições de recursos computacionais. Por este motivo tem sido utilizado em redes *ad-hoc* e, agora, se propõe empregá-lo em documentos eletrônicos assinados por meio do Certificado Otimizado, tema do Capítulo 4.

Entrada: S_k, X_n, Y_1, F
Saída: Validade do certificado
início
  se $F^k(S_k) = X_n$ **então**
    "certificado válido"
  senão
    se $F^1(S_k) = Y_1$ **então**
      "certificado revogado"
    senão
      "indefinido"
    fim
  fim
fim

Algoritmo 1: Verificação da validade de certificado segundo Novomodo

3.6.2 Síntese dos Trabalhos Relacionados

Os trabalhos relacionados serviram de base para a elaboração da Infraestrutura de Chaves Públicas Otimizadora (Capítulo 4). Eles foram combinados e estendidos neste trabalho como se descreve a seguir.

Consideraram-se os certificados aninhados com o objetivo de reduzir o número de operações criptográficas durante a validação do caminho de certificação. Assim, utilizou-se a ideia de emitir um Certificado Otimizado para um certificado convencional. Entretanto, no presente trabalho sugere-se a validação convencional de caminho de certificação sem comparações entre resumos criptográficos como sugere [14]. Ainda, ao se emitir um Certificado Otimizado para um convencional, copia-se a chave pública do segundo, de forma que o primeiro possa verificar assinaturas digitais criadas pela chave privada relacionada ao segundo.

A proposta de Certificado Otimizado é combinada com o conceito de verificadores. Propõe-se, então, a Autoridade Certificadora de Certificados Otimizados. Trata-se de um serviço notarial de verificação de certificados convencionais que, em paralelo, emite Certificados Otimizados.

Este trabalho estende a proposta de certificado de curta duração. Propõe-se que o prazo de validade do Certificado Otimizado seja um instante particular ao invés de um breve período de tempo. Desta maneira elimina-se qualquer possibilidade de revogação bem como permite-se usar o Certificado Otimizado como carimbo do tempo de uma informação qualquer (e.g. a assinatura digital sobre o documento eletrônico).

Por fim, utiliza-se o método Novomodo na Infraestrutura de Chaves Públicas Otimizadora. Todavia, sugere-se integrá-lo com uma entidade mediadora, denominada *Crypto Time*, para que o Novomodo possa

ser utilizado a baixo custo por uma AC Raiz. Adicionalmente, apresenta-se um esquema de *logs* seguros combinado as informações do Novomodo.

3.7 CONCLUSÃO

Este capítulo apresentou a validação de documentos eletrônicos assinados destacando a verificação da irretratabilidade da assinatura digital. Tal processo requer descobrir, localizar e validar os certificados e informações de revogação presentes no caminho de certificação do signatário, tarefa que exige recursos computacionais de processamento, armazenamento e comunicação.

Diferentemente de uma assinatura de próprio punho, viu-se que uma assinatura digital tem um prazo de validade limitado, seja pelo enfraquecimento dos algoritmos criptográficos ou pela validade finita de um certificado digital. Não obstante, demonstrou-se que a validade de uma assinatura digital pode ser estendida indeterminadamente através da adição de carimbos do tempo. Contudo, carimbos do tempo são documentos eletrônicos assinados que demandam validação, contribuindo para aumentar a dificuldade do uso de certificação digital.

Destacou-se também os problemas relativos as LCRs e OCSP. De fato, considera-se a consulta à situação de revogação de certificados um dos obstáculos ao uso em larga escala de documentos eletrônicos assinados [71]. Isso se deve à dificuldade em se efetuar o processo de verificação de revogação, para o qual ainda não existe uma solução de alta performance e cujas informações sejam atualizadas em tempo real [72].

Apresentaram-se os trabalhos presentes na literatura que buscam mitigar as dificuldades do uso de certificação digital para documentos eletrônicos. Por fim, descreveu-se como tais trabalhos foram integrados e estendidos em uma nova solução: a Infraestrutura de Chaves Públicas Otimizadora, apresentada no capítulo a seguir.

4 CERTIFICAÇÃO DIGITAL OTIMIZADA PARA DOCUMENTOS ELETRÔNICOS

4.1 INTRODUÇÃO

Ao longo do Capítulo 3 foram apresentadas dificuldades para se usarem serviços de ICP. Por exemplo, o esforço computacional para tratar os dados de validação de assinaturas digitais sobre documentos eletrônicos. Para minimizar esses esforços propõem-se neste capítulo o Certificado Otimizado e a Infraestrutura de Chaves Públicas Otimizadora.

O restante deste capítulo está organizado da seguinte forma. A Seção 4.2 introduz os conceitos de Certificados Otimizados, úteis para a otimização de dados de validação. Para a emissão dos Certificados Otimizados há a Autoridade Certificadora de Certificados Otimizados (ACCO), apresentada na Seção 4.3. Em seguida, na Seção 4.4 descreve-se o mecanismo de revogação para o certificado da ACCO. Na Seção 4.5 expõe-se um sistema de registros seguros para a ACCO, de modo que esta possa ser auditada. Na Seção 4.6 explica-se a validação de documentos eletrônicos assinados e otimizados. A seção 4.7 aborda o emprego da ACCO em um domínio de usuários de documentos eletrônicos assinados. A Seção 4.8 mostra como os Certificados Otimizados podem beneficiar entidades arquivísticas. Unindo os conceitos apresentados nas seções anteriores, a Seção 4.9 apresenta a Infraestrutura de Chaves Públicas Otimizadoras. Por fim, a Seção 4.10 conclui este capítulo.

4.2 CERTIFICADO OTIMIZADO

Para reduzir o esforço computacional necessário para a verificação da assinatura digital sobre um documento eletrônico propõe-se otimizar os dados de validação do signatário, como ilustra a Figura 4.1. A otimização proposta, que pode ser realizada tanto pelo signatário como pelo verificador de um documento eletrônico assinado, consiste em reduzir o volume de dados de validação, substituindo o caminho de certificação do signatário, informações de revogação e carimbos do tempo pelo caminho de certificação otimizado. Este é composto por apenas dois certificados: o Certificado Otimizado (CO) e o certificado da Autoridade Certificadora de Certificados Otimizados (ACCO). Nota-se, entretanto, que esse processo preserva o documento eletrônico e a assinatura digital criada pelo signatário.

A substituição dos dados de validação é possível porque o CO é capaz de verificar a assinatura digital. Isto ocorre devido ao CO ter campos cujos valores são equivalentes aos do certificado do signatário, como ilustra a Figura 4.2. Nesta, observa-se que os campos do CO *Version*, *Sig-*

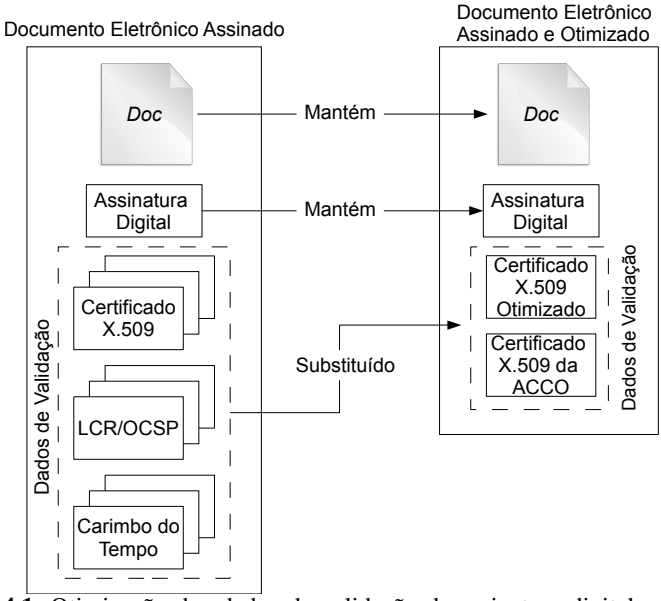

Figura 4.1: Otimização dos dados de validação da assinatura digital sobre um documento eletrônico.

nature Algorithm, *Subject*, *Subject Key Info* e *Extensões Arbitrárias*, cuja cor de fundo é branca, são cópias dos campos do certificado do signatário. Já os demais campos, cuja a cor de fundo é cinza, possuem valores distintos e pertencentes escopo do CO.

Percebe-se, na Figura 4.2 que os campos *NotBefore* e *NotAfter* possuem o mesmo valor. Esta equivalência proposital faz do CO um certificado de curta-duração como proposto Rivest [15], porém com uma sutil diferença: a validade do CO é um instante de tempo i, correspondente a sua data de emissão. Devido a esta característica particular, não há razão em se revogar um CO, pois se ele foi emitido, então ele era válido no momento da emissão. Por esse motivo, os dados de validação otimizados não incluem informação de revogação para o CO.

Além de reduzir as informações de revogação, a validade do CO permite acrescentar-lhe outra funcionalidade: a de carimbo do tempo. Portanto, inclui-se o resumo criptográfico de uma assinatura digital sobre o documento eletrônico. Esta funcionalidade é implementada através da inclusão de uma extensão X.509, representada pelo objeto *Extensões para ICPO* na Figura 4.2. Adicionalmente, essa inclusão atrela o CO a uma assinatura digital arbitrária, impedindo que o CO possa ser utilizado com outras assinaturas produzidas pelo mesmo signatário.

Contudo, a substituição dos dados de validação permitiria ocultar dos verificadores de documentos eletrônicos assinados informações im-

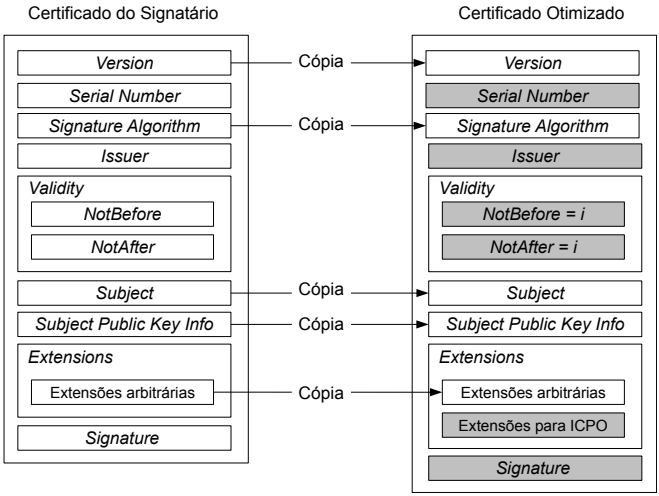

Figura 4.2: Comparação entre o certificado digital do signatário e o CO.

portantes, como por exemplo, a revogação de algum certificado no caminho de certificação do signatário. Portanto, semelhante aos Certificados Aninhados, define-se que a emissão do CO deva ser precedida pela completa verificação do caminho de certificação do signatário a partir dos dados de validação originais. Consequentemente, o CO representa um atestado de que, no momento de sua emissão, validou-se com sucesso o caminho de certificação do signatário.

Por fim, para dar suporte a emissão do CO faz-se a inclusão de um novo serviço à ICP, o qual deve ser confiável e capaz de verificar caminhos de certificação. Para esta tarefa designa-se a Autoridade Certificadora de Certificados Otimizados (ACCO), apresentada a seguir.

4.3 AUTORIDADE CERTIFICADORA DE CERTIFICADOS OTIMIZADOS

A ACCO opera como um serviço notarial *online* alocado estrategicamente dentro de uma ICP. A ACCO exerce, simultaneamente, os papéis de verificador e de Autoridade de Carimbo do Tempo. Portanto, sua função é verificar o caminho de certificação de um signatário, emitindo um CO que atesta, na data de emissão, a existência de uma assinatura digital sobre um documento eletrônico bem como a validade do certificado do signatário.

Qualquer usuário, seja ele o signatário ou um verificador de um documento eletrônico assinado, pode solicitar um CO. Assim, para ilustrar a interação com a ACCO apresenta-se a Figura 4.3. Nesta, observa-se que o usuário submete: a) o resumo criptográfico da assinatura digital sobre o documento eletrônico assinado, ilustrado por *F(Assinatura Digital)*

na figura; b) o caminho de certificação do signatário; c) informações de revogação; e c) uma referência temporal na qual o usuário concorda com a assinatura sobre o documento eletrônico (e.g. um carimbo do tempo, incluindo dados de validação). Em seguida, a ACCO verifica o caminho de certificação do signatário e os carimbos do tempo, e caso sejam válidos, emite um CO. Este e o certificado da ACCO constituem o caminho de certificação otimizado – também denominado dados de validação otimizados –, que é enviado ao usuário. Por fim, de posse desses dados o usuário efetua o processo de otimização ilustrado na Figura 4.1.

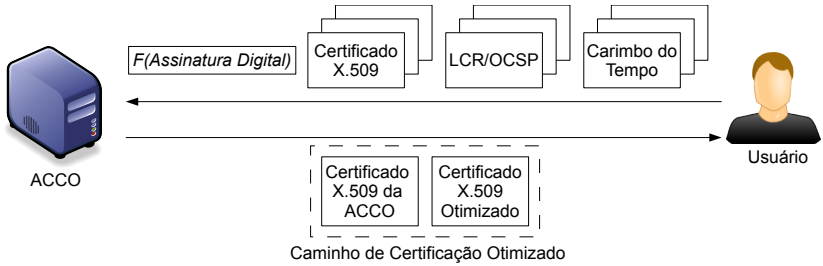

Figura 4.3: Processo de requisição e emissão de Certificados Otimizados.

Para verificar o caminho de certificação do signatário, a ACCO pode utilizar diferentes referências temporais, como apresenta a Tabela 4.1. No primeiro caso ($N = 1$) a validação é efetuada no instante da requisição do CO e utilizam-se a data e hora correntes do relógio interno da ACCO. Em $N = 2$, caso da Figura 4.3, a validação ocorre no instante informado por um carimbo do tempo (e.g. sobre assinatura do documento ou sobre referências de validação). Em $N = 3$ a referência de tempo equivale ao momento em que a assinatura foi criada e, neste caso, o solicitante do CO deve se identificar como signatário do documento eletrônico, por exemplo, através de um protocolo de desafio-resposta (e.g. [73]) . Por fim, em $N = 4$ a referência é informada por um verificador, correspondendo a um momento no passado em que ele concordava com a assinatura do documento.

Tabela 4.1: Referência e fonte de tempo para validação de assinatura digital.

N	Referência	Fonte
1	Instante da requisição do CO	Relógio interno da ACCO
2	Instante passado	Carimbo de tempo
3	Instante passado	Signatário do documento
4	Instante passado	Verificador do documento

Com exceção dos casos em que $N = 1$ e $N = 2$, é possível que uma revogação no caminho de certificação do signatário possa ser ocultada da ACCO, que emitiria um CO otimizado válido. Isto ocorre pois tanto o signatário quanto o verificador poderiam escolher uma data anterior a revogação, quando o caminho de certificação ainda era válido. Por

este motivo, julga-se interessante que o CO informe aos verificadores a referência temporal utilizada pela ACCO. Esta informação é contemplada através da inclusão de uma extensão X.509, representada pelo objeto *Extensões para ICPO* na Figura 4.2.

O caminho de certificação otimizado (Figura 4.3) deve ter o menor comprimento possível a fim de que o volume de dados de validação seja mínimo. Para alcançar este objetivo plenamente, a ACCO deveria ser um serviço da AC-Raiz de uma ICP. Ou seja, a própria AC-Raiz emitiria COs. Contudo, tal prática é desencorajada pois se aumentariam os custos operacionais já elevados de uma AC Raiz, a qual deveria permanecer *online* e, consequentemente, estaria exposta a ataques pela rede. Portanto, sugere-se que a ACCO seja subordinada diretamente à AC-Raiz.

Por fim, a subordinação direta da ACCO à AC Raiz lança um novo desafio: a gerência das informações de revogação para a ACCO. Haja vista que esta é um serviço *online* e, portanto, exposto a ataques, é prudente que a situação de revogação seja atualizada frequentemente. Entretanto, tal tarefa pode esbarrar na frequência de operação da AC Raiz, a qual é normalmente mantida desligada e isolada na maior parte do tempo por motivos de segurança e de custos operacionais. Para superar este desafio apresenta-se a seguir uma adaptação do método de revogação Novomodo.

4.4 MECANISMO DE REVOGAÇÃO NO CAMINHO DE CERTIFICAÇÃO OTIMIZADO

Diferente do CO, o certificado da ACCO possui um prazo de validade convencional. Por exemplo, 3 anos, semelhante a uma Autoridade de Carimbo do Tempo na ICP-Brasil [74]. Portanto, é necessário que se adote um mecanismo de revogação, mas diferenciado para que não se enfrentem os problemas apontados no Capítulo 3 (e.g. LCRs longas). Deste modo, opta-se por utilizar o eficiente método Novomodo.

Com o objetivo de exigir o mínimo de interação com o responsável pela publicação da situação de revogação para a ACCO, ou seja, a AC Raiz, apresenta-se o *Crypto Time*. Trata-se de um serviço *online* acrescentado a ICP cujo objetivo é manter sob sigilo informações de revogação do Novomodo e apenas torná-las públicas (e.g. através de um repositório ou diretório públicos) quando autorizado.

Primeiro, a AC Raiz produz, previamente, as provas de validade (X_{n-k}, para $0 < k < n$) que poderão ser publicadas durante o período de validade de uma nova ACCO. Logo após a AC Raiz emitir o certificado da ACCO, as provas de validade são transferidas de maneira segura ao *Crypto Time* (e.g. cifrando os dados com a chave pública do *Crypto Time*), que deverá mantê-las sob sigilo. Ao longo da vida da ACCO as provas serão liberadas gradativamente pelo *Crypto Time*, mediante prévia autorização de auditores da ICP que atestarão periodicamente a integridade da ACCO. Percebe-se, portanto, que os valores úteis para sinalizar

revogação (Y_0 e Y_1) não são utilizados.

Verificadores averiguam a situação de revogação da ACCO por meio do Algoritmo 2, cujos valores de entrada são: a prova de validade (X_{n-k}), o alvo de validade (X_n), a função de resumo criptográfico F, o total de publicações de situação de revogação durante o tempo de vida da ACCO (n) e o número da publicação atual (k). Com exceção de X_{n-k}, que é publicado pelo *Crypto Time*, os demais valores estão presentes no certificado da ACCO.

Entrada: X_{n-k}, X_n, F, n, k
Saída: Validade do certificado
início
  se $F^k(X_{n-k}) = X_n$ **então**
    "certificado válido"
  senão
    "X_{n-k} é inválido"
  fim
fim

Algoritmo 2: Algoritmo Novomodo simplificado.

A ausência da verificação dos valores que sinalizam revogação (Y_0 e Y_1) no Algoritmo 2 é justificada pelos papéis do *Crypto Time* e dos auditores. Caso os auditores decidam revogar o certificado da ACCO durante a k-ésima publicação de situação de revogação, a prova de validade X_{n-k} não é liberada pelo *Crypto Time*. A ausência de X_{n-k} causa o bloqueio das operações da ACCO imediatamente após a expiração da prova de validade anterior ($X_{n-(k-1)}$). Além disso, descarta-se a possibilidade de se obter X_{n-k} a partir de $X_{n-(k-1)}$, fato sustentado pela inviabilidade computacional da inversão de funções de resumo criptográfico.

Em suma, o *Crypto Time* é um serviço adicional a uma ICP, cuja função é servir de mediador entre a entidade que produz as informações de revogação e seus respectivos interessados. Por exemplo, verificadores de assinaturas digitais sobre documentos eletrônicos assinados. Desta forma, o *Crypto Time* retira da AC Raiz a responsabilidade de publicar as situações de revogação.

Por fim, vale mencionar novamente que a liberação das provas de validade pelo *Crypto Time* é precedida pela auditoria da ACCO, de forma a comprovar sua integridade. Para auxiliar os auditores nesta função, apresenta-se a seguir um sistema de registro de atividades seguro para a ACCO.

4.5 SISTEMA DE REGISTROS SEGURO

Como mencionado anteriormente, um sistema de registros de atividades para a ACCO tem o objetivo de subsidiar os auditores com informações sobre a integridade da ACCO. Por exemplo, evidências de que chave privada foi comprometida. Ainda, é desejável que esses sistemas sejam protegidos, de modo que, no mínimo, evidenciem tentativas de adulterações nos registros. Como exemplos de soluções para tal requisito de segurança podem-se citar os *logs* auditáveis para computação forense [75] e o carimbo do tempo relativo [76], sendo este último utilizado neste trabalho.

A escolha pelo carimbo do tempo relativo se deu por dois motivos. O primeiro porque se podem encadear os COs, criando-se uma sequência que define a ordem de emissão dos COs. Ainda, podem-se publicar pontos desta sequência, evitando que um adversário a adultere sem que os auditores percebam.

O segundo motivo está na possibilidade de se combinar o carimbo do tempo relativo com as provas de validade (X_{n-k}) do Novomodo. Desta forma podem-se identificar, quando do comprometimento da ACCO, quais COs foram emitidos enquanto a ACCO era íntegra. Caso não haja um mecanismo que permita classificar os COs, todos estes passam a ser considerados inválidos a partir da revogação da ACCO, de maneira similar aos carimbos do tempo após a revogação de uma ACT. Sem dúvida, esta é uma situação crítica para uma ICP e seus usuários.

Propõe-se, então, que a ACCO mantenha, ao longo de sua vida, uma sequência única que contém o resumo criptográfico de cada CO emitido. Tal sequência é segmentada em $\frac{n}{l}$ períodos, sendo n e l as variáveis do método Novomodo explicadas na Seção 3.6.1. Cada período k, sendo $0 \leq k < \frac{n}{l}$, inicia com a inserção da prova X_{n-k} na sequência, seguida dos resumos criptográficos de cada CO emitido durante o prazo de validade de X_{n-k}.

Todo CO é atrelado ao seu antecessor. Assim, em cada certificado otimizado $CO_{j,k}$ ($j \geq 0$) emitido durante k, embarcam-se, através de uma extensão X.509, X_{n-k} para $j = 0$ e o resumo criptográfico de $CO_{j-1,k}$ para $j > 0$.

As provas X_{n-k} são atreladas ao último CO emitido durante o período $k - 1$ antes de serem inseridas na sequência, de modo a estabelecer o final desse período. Portanto, para $k \geq 1$, relaciona-se X_{n-k} ao último CO no período $k - 1$. Para $k = 0$ utiliza-se a prova X_n sem relacioná-la a outro dado.

A Figura 4.4 ilustra esse encadeamento de COs através de quatro períodos de comprimento l. O primeiro período ($k = 0$) inicia-se com X_n. Em seguida CO_1 é emitido com X_n embarcado, logo CO_2 é emitido com o resumo criptográfico $F(CO_1)$ embarcado. Imediatamente após o segundo período iniciar ($k = 1$) insere-se $F(F(CO_x)||X_{n-1})$ – resumo criptográfico calculado sobre a concatenação de $F(CO_x)$ e X_{n-1} –, de

modo a estabelecer o fim do primeiro período ($k = 0$). O mesmo processo de amarração entre COs é repetido em $k = 2$ e $k = 3$. Nota-se que em $k = 4$ a ACCO não consegue emitir novos COs, pois seu certificado expirou, bem como a falta da última prova de validade impede a emissão de novos COs. Por fim, a sequência é fechada através da inclusão do valor Novomodo X_0.

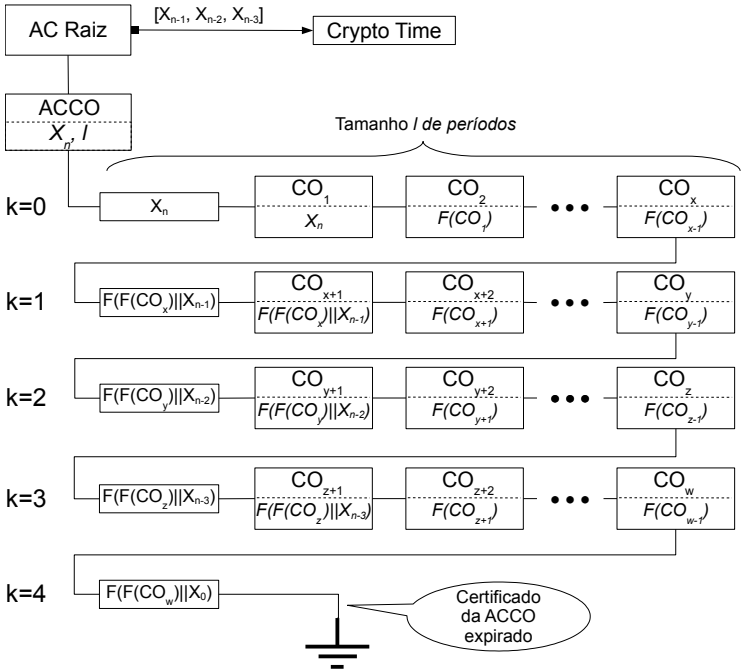

Figura 4.4: Encadeamento entre COs e dados do método Novomodo.

Em suma, o sistema de registro proposto subsidia os auditores com informações sobre as operações da ACCO. Adicionalmente, o uso combinado do carimbo do tempo relativo com as provas X_{n-k} proporciona informação adicional a um CO, permitindo que se identifique em qual dos $\frac{n}{l}$ períodos ele foi emitido. Tal informação pode viabilizar medidas eficientes para contingenciar a revogação da ACCO, ao invés de se invalidarem todos os COs emitidos, inclusive aqueles genuínos.

Sugere-se também que se repliquem os COs emitidos em repositórios. Desta forma, caso um adversário tente regerar toda a sequência de resumos criptográficos mantida pela ACCO, os auditores poderiam perceber a fraude, desde que verifiquem se a cadeia condiz com os COs emitidos no passado.

Por fim, lembra-se que, embora as informações de carimbo do tempo relativo estejam disponíveis nos COs, estas não são úteis aos usuário no momento da verificação da assinatura digital sobre um do-

cumento eletrônico. Este processo, por sua vez, é explicado a seguir.

4.6 VERIFICAÇÃO DA ASSINATURA DIGITAL SOBRE UM DOCUMENTO ELETRÔNICO

A verificação da assinatura digital sobre um documento eletrônico, cujos dados de validação foram otimizados, ocorre de maneira similar à certificação digital convencional. Entretanto, no final da validação cabe ao verificador confiar na veracidade do CO. Esse processo é realizado de acordo com os seguintes passos.

O primeiro passo consiste em verificar a integridade e autenticidade da assinatura digital sobre o documento eletrônico. Esta etapa é realizada através do uso da chave pública do signatário, que se encontra disponível no CO.

No segundo passo, o verificador deve verificar a validade do caminho de certificação otimizado. Para isso ele executa o algoritmo *Certificate Path Processing* utilizando como referência temporal o instante de emissão do CO. Em seguida, o verificador acessa o repositório ou diretório público do *Crypto Time* e busca a prova X_{n-k} do período atual k. Caso a prova não esteja disponível, concluí-se que a ACCO foi revogada e não se pode garantir a validade da assinatura digital. Caso contrário, o verificador obtém a prova e executa o Algoritmo 2. Se este sinalizar a validade do certificado da ACCO, então a assinatura digital é válida. Senão, não se pode garantir a validade do certificado, dado que o valor de X_{n-k} é inválido para o período k.

Sabe-se que o CO representa um atestado de que o caminho de certificação do signatário foi validado pela ACCO. Não obstante, o usuário de documentos eletrônicos assinados pode questionar a veracidade de um CO. Neste caso, sugere-se considerar: a) o situação de revogação da ACCO e a referência temporal (Tabela 4.1), ou seja, se a ACCO não foi comprometida e se a mesma utilizou uma referência temporal segura (e.g. o relógio interno da ACCO ou um carimbo do tempo), então se espera que o CO seja genuíno; ou b) verificar o caminho de certificação do signatário. Nesta alternativa, o usuário iria conferir a verificação efetuada pela ACCO, por exemplo, na primeira vez em que utilizasse o documento eletrônico assinado. Nas ocasiões seguintes, o usuário poderia utilizar os dados de validação otimizados, economizando recursos computacionais.

Por fim, percebe-se que a certificação otimizada não elimina os dados de validação convencionais, para os quais os verificadores podem recorrer sempre que julgarem necessário. A seguir apresenta-se um cenário em que se ilustra o emprego da ACCO cujos COs emitidos coexistem com os certificados X.509 convencionais.

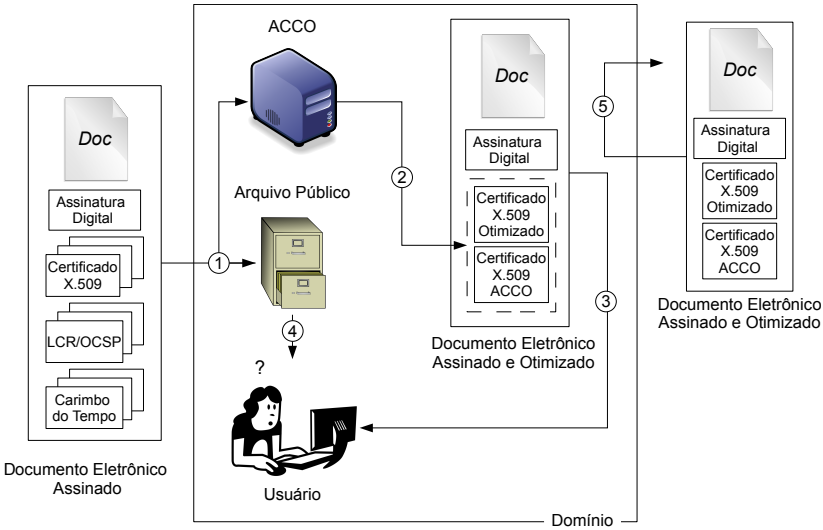

Figura 4.5: Emprego da ACCO em um domínio de usuários.

4.7 EMPREGO DA ACCO

Como mencionado anteriormente, a ACCO é um serviço notarial *online* cuja função é emitir COs, úteis para reduzir os dados de validação de um documento eletrônico assinado e, consequentemente, diminuir o uso de recursos computacionais. De forma a exemplificar seu uso, ilustra-se o cenário a seguir.

Um domínio de usuários de documentos eletrônicos assinados deseja economizar recursos. Portanto, há um consenso entre os usuários sobre utilizar documentos assinados e otimizados sempre que possível. Todo documento eletrônico assinado que ingressa no domínio passa pelo processo ilustrado na Figura 4.5. Em 1 guarda-se no Arquivo Público uma cópia dos dados de validação da assinatura digital sobre documento eletrônico e se solicita um CO à ACCO. Em 2, otimiza-se o documento eletrônico assinado, substituindo-se os dados de validação originais pelo caminho de certificação otimizado. Em 3 o documento eletrônico assinado e otimizado torna-se disponível aos usuários do domínio.

Antes de utilizar um documento eletrônico assinado e otimizado, o usuário verifica a assinatura digital e valida o caminho de certificação otimizado. Caso o usuário confie na veracidade do CO, nenhuma verificação adicional precisa ser feita. Caso contrário, em 4 o usuário solicita os dados de validação originais ao Arquivo Público e os valida, constatando a veracidade do CO. A partir desse momento, o passo 4 não será mais necessário em futuros usos do documento eletrônico assinado e otimizado.

Em 5 ilustra-se a ocasião em que se rejeita a entrada de um documento eletrônico assinado e otimizado cujo CO foi emitido por uma

ACCO desconhecida. Isso ocorre pois nesse domínio decidiu-se por não se confiar em ACCOs externas, haja vista que não estão disponíveis os dados de validação originais para se confirmar a veracidade do CO.

Uma vez que usuários externos ao domínio podem desconhecer a ACCO, sugere-se desfazer a otimização de um documento eletrônico assinado antes de enviá-lo para fora do domínio. Dessa maneira, cabe ao usuário solicitar ao Arquivo Público os dados originais de validação e, em seguida, anexá-los ao documento eletrônico assinado, removendo o caminho de certificação otimizado.

Finalmente, nota-se que o uso do CO para otimizar os dados de validação em documentos eletrônicos assinados permite a redução do esforço computacional do usuário. Do ponto de vista do domínio, a economia de recursos é mais expressiva, uma vez que um mesmo documento assinado pode ser verificado diversas vezes por diferentes usuários. Sabe-se também que diversas cópias do mesmo documento eletrônico assinado podem circular dentro do domínio, havendo redundância de dados de validação. Ainda, caso estes não sejam otimizados, o impacto da manutenção da autenticidade da assinatura digital nos recursos do domínio será multiplicado pelo número de cópias.

4.8 BENEFÍCIOS PARA ARQUIVAMENTO A LONGO PRAZO

O emprego de COs apresenta atraentes benefícios para assinaturas que precisam ser verificáveis por longos períodos. Tais assinaturas são geralmente preservadas através da adição de sucessivos carimbos do tempo, como no CAdES-A, XAdES-A [55] e *Evidence Record Syntax* (ERS) [77]. Entretanto, a quantidade crescente de carimbos incide diretamente na demanda por recursos de armazenamento e de processamento: um obstáculo para o uso de documentos assinados em ambientes cujos recursos são restritos.

Com o passar do tempo tanto os carimbos do tempo como os COs estão sujeitos a problemas de expiração de caminho de certificação e enfraquecimento dos algoritmos criptográficos utilizados. Por exemplo, algoritmos de resumo criptográficos tornam-se inseguros a partir do momento em que suas propriedades (Seção 2.2) não podem ser garantidas perante o poder computacional existente. Entretanto, ao contrário de um carimbo do tempo, um CO pode ser facilmente substituído por outro CO de nova validade e cuja assinatura foi criada através de um algoritmo criptográfico mais forte. Desta maneira, obtém-se um esquema de preservação por longo prazo com requisitos mínimos e relativamente constantes na validação das assinaturas digitais.

4.9 INFRAESTRUTURA DE CHAVES PÚBLICAS OTIMIZADORA

Uma vez apresentados todos os conceitos envolvidos na certificação otimizada, apresenta-se a Infraestrutura de Chaves Públicas Otimizadora (ICPO). Esta corresponde a uma ICP convencional em que se adiciona uma ou mais Autoridades Certificadoras de Certificados Otimizados. Portanto, na ICPO certificados X.509 convencionais e otimizados coexistem normalmente. Ainda, na ICPO existem mecanismos de revogação comuns (e.g. LCRs e OCSP) bem como o método Novomodo, que conta com o suporte do *Crypto Time*. Para a ilustrar a ICPO e os conceitos envolvidos, apresenta-se a Figura 4.6.

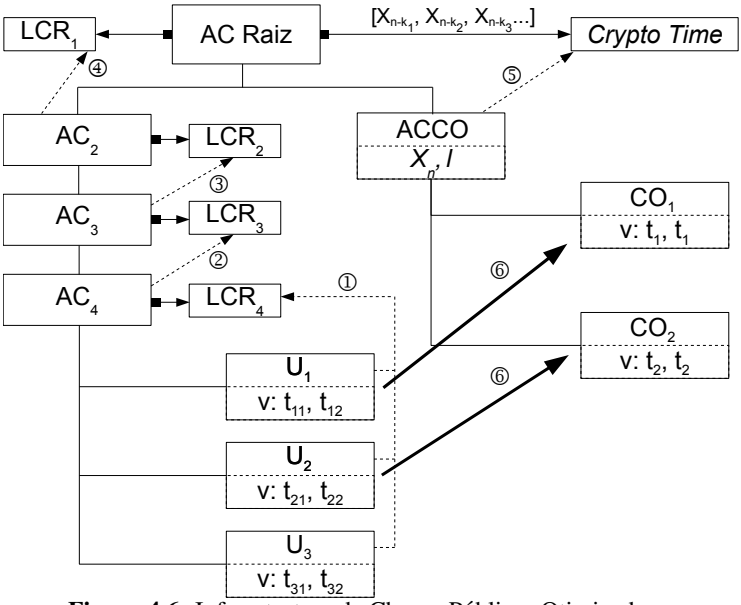

Figura 4.6: Infraestrutura de Chaves Públicas Otimizadora.

Observa-se na Figura 4.6 uma hierarquia de certificados cujo topo é ocupado pela AC Raiz. No ramo esquerdo, abaixo da AC Raiz, estão os certificados X.509 convencionais AC_2, AC_3, AC_4, U_1, U_2 e U_3. Os três primeiros certificados pertencem a Autoridades Certificadoras, enquanto os demais a usuários finais. Adicionalmente, as setas de linha pontilhada e numeradas de 1 a 5 destacam, para cada certificado mencionado, sua respectiva informação de revogação. Por exemplo, a situação de revogação de U_1 é encontrada na LCR_4. Ainda, cada LCR é vinculada, por meio de uma seta, ao seu emissor. Por exemplo, a LCR_1 é emitida pela AC Raiz, enquanto LCR_2 pela AC_2.

À direita da hierarquia estão os serviços para certificação digital otimizada. Observa-se que a AC Raiz gera as provas de validade Novo-

modo ([X_{n-k_1},X_{n-k_2},X_{n-k_3}...]) e as envia para o *Crypto Time*. Abaixo da AC Raiz está a ACCO, que obtém sua situação de revogação no *Crypto Time*, como destaca a seta 5, de linha pontilhada. A ACCO, por sua vez, emite os Certificados Otimizados CO_1 e CO_2.

Por fim, percebe-se que Figura 4.6 destaca, através das setas 6, a otimização do caminho de certificação de U_1 e U_2, cujo resultado são CO_1 e CO_2. Nota-se também que, por serem certificados X.509 convencionais, U_1, U_2 e U_3 têm seus prazos de validade delimitados por instantes distintos. Por exemplo, o prazo de validade de U_1 inicia em t_{11} e finaliza em t_{12}. Por outro lado, os Certificados Otimizados CO_1 e CO_2 são válidos por apenas um instante de tempo. Por exemplo, CO_1 é válido apenas para o instante t_1

4.10 CONCLUSÃO

Este capítulo apresentou a Infraestrutura de Chaves Públicas Otimizadora. Trata-se de uma ICP convencional em que foi acrescentado um novo serviço: a Autoridade Certificadora Otimizadora (ACCO). Esta é um verificador ou notário *online* que permite usuários reduzir o volume de dados de validação para assinatura digitais presentes em documentos eletrônicos assinados. Para tal, os usuários submetem os dados de validação para a ACCO, que os valida e emite um atestado de validade: o Certificado Otimizado (CO). Este é, então, utilizado pelos usuários para substituir os dados de validação, reduzindo os esforços computacionais para verificar e manter a autenticidade a longo prazo de assinaturas digitais sobre documentos eletrônicos.

Para garantir que o caminho de certificação do CO seja mais simples de verificar e ocupe menos espaço que um caminho de certificação convencional, lança-se mão de diversos artifícios. Primeiro, o CO é válido por um instante particular de tempo. Portanto, dispensa verificação situação de revogação. Segundo, o caminho de certificação otimizado tem comprimento curto, composto apenas pelo CO e o certificado da ACCO. Terceiro, usa-se o eficiente método de revogação Novomodo para verificar a situação de revogação da ACCO. Quarto, o CO substitui carimbos do tempo, reduzindo ainda mais os dados de validação.

Por fim, um CO, cujo caminho de certificação deixará de ser válido devido à expiração do certificado da ACCO ou obsolescência de algoritmo criptográfico, pode ser facilmente substituído por um novo CO. Este artifício é extremamente atraente para a manutenção a longo prazo da autenticidade de assinaturas digitais sobre documentos eletrônicos, uma vez que não incrementa o volume de dados de validação.

5 IMPLEMENTAÇÃO DE PROTÓTIPO

5.1 INTRODUÇÃO

A implementação de protótipo de aplicações para simular a Infraestrutura de Chaves Públicas Otimizadora tem o objetivo de testar o funcionamento certificação digital otimizada para documentos na prática. Desta forma, podem-se localizar erros na proposta e, principalmente, verificar a compatibilidade dos Certificados Otimizado com aplicações existentes.

Para o desenvolvimento do protótipo foi escolhida a linguagem de programação Java [78]. Esta escolha considerou o conhecimento do autor sobre a linguagem e, principalmente, sobre a biblioteca criptográfica denominada *Bouncy Castle* [79]. Juntas, estas ferramentas proporcionam uma solução completa para criação de aplicações voltadas a ICP.

O restante deste capítulo é organizado da seguinte forma. A Seção 5.2 apresenta a implementação do Certificado Otimizado a partir do padrão X.509. A Seção 5.3 descreve a otimização, através do Certificado Otimizado, de um documento assinado no formato PKCS#7. A Seção 5.4 apresenta dois protótipos de aplicações: a) um cliente para criar, verificar e otimizar documentos eletrônicos; e b) um servidor, para gerir uma Autoridade Certificadora de Certificados Otimizados. Por último, a Seção 5.5 apresenta a implementação do *Crypto Time*.

5.2 CERTIFICADO OTIMIZADO

A implementação de CO fez uso dos artefatos da linguagem Java que geram e abstraem certificados X.509. Assim, para emitir de um CO usou-se o artefato gerador certificados X.509, que recebeu um prazo de validade cujo início e fim possuíam o mesmo valor (i.e. *notBefore=nofAfter*), e um conjunto de extensões X.509. Estas foram necessárias para se embarcarem nos certificados X.509 informações pertinentes à certificação otimizada.

A Figura 5.1 ilustra o Certificado Otimizado. Pode-se observar que se trata de um certificado X.509 cujos os campos são apresentados na Página 19. Entretanto, o prazo de validade (campo *Validity*) é adaptado para representar um instante de tempo e o campo *Extensions* contém extensões arbitrárias.

As extensões X.509 foram definidas na linguagem ASN.1 [1] e, em seguida, implementadas por meio de artefatos Java responsáveis por codificá-las de acordo com regras binárias (e.g. *Distinguished Encoding Rules* [80]). As figuras 5.2, 5.3, 5.4 e 5.5 ilustram a definição em ASN.1 do resumo criptográfico da assinatura digital sobre documento eletrônico, o

[1] Linguagem de definição de dados padronizada pela ISO [47]

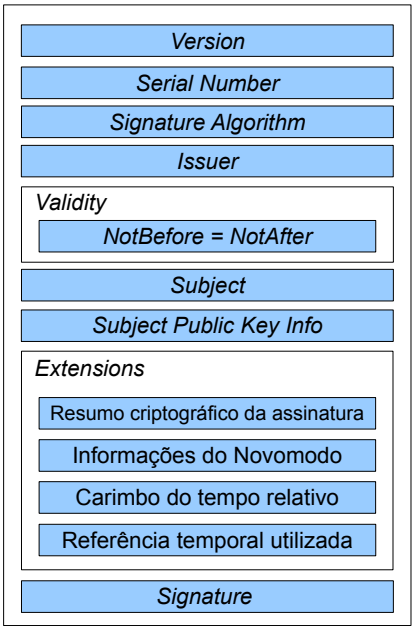

Figura 5.1: Certificado Otimizado.

carimbo do tempo relativo, as informações do Novomodo (F, X_n, X_{n-k} e l) e a referência temporal utilizada pela ACCO para validar a assinatura sobre um documento eletrônico.

```
SEQUENCE {
    digestAlgorithm AlgorithmIdentifier, --importado de RFC5280
    documentDigest  BIT STRING
    }
```

Figura 5.2: Extensão X.509 para resumo criptográfico da assinatura digital sobre um documento eletrônico

5.3 OTIMIZAÇÃO DE DOCUMENTOS ELETRÔNICOS ASSINADOS

A otimização de documentos eletrônicos assinados consiste em substituir os dados de validação da assinatura (certificado e caminho de certificação do signatário, LCRs e carimbos do tempo) pelo caminho de certificação otimizado. Este processo é efetuado sobre uma assinatura digital no formato PKCS#7, cujo modelo conceitual é ilustrado na Figura 5.6.

```
SEQUENCE {
    digestAlgorithm AlgorithmIdentifier, --importado de RFC5280
    previous  BIT STRING
    }
```

Figura 5.3: Extensão X.509 para carimbo do tempo relativo

```
SEQUENCE {
    digestAlgorithm [0] AlgorithmIdentifier, --importado de RFC5280
    validityTarget  [1] BIT STRING,
    validityProof   [2] BIT STRING OPTIONAL,
    granularity     [3] INTEGER
    }
```

Figura 5.4: Extensão X.509 para informações do Novomodo

```
ENUMERATE {
    occaClock(1), timeStamp(2), signer(3), verifier(4)
    }
```

Figura 5.5: Extensão X.509 para referência temporal utilizada pela ACCO na verificação da assinatura sobre um documento eletrônico.

Nesse modelo conceitual define-se um elemento central (*PKCS#7*), o qual pode incluir: zero ou mais certificados; zero ou mais LCRs e um ou mais signatários, os quais assinam um documento eletrônico representado por *infoConteúdoEncap*. No elemento *InfoSignatário* estão presentes a assinatura digital, a identificação do signatário (*idSignatário*) e zero ou mais carimbos do tempo.

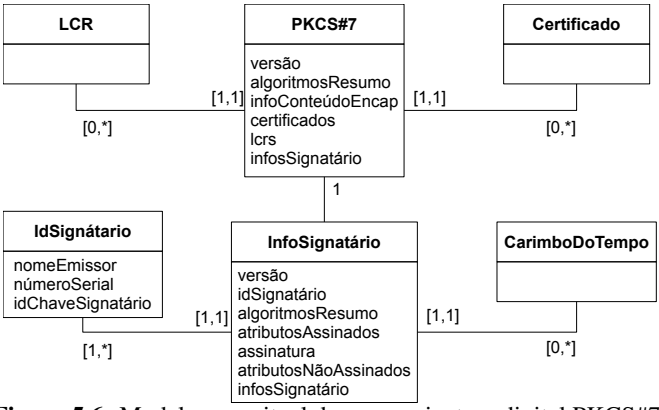

Figura 5.6: Modelo conceitual de uma assinatura digital PKCS#7.

Dado um signatário do documento eletrônico assinado, a otimização consiste em remover todas as ocorrências de *Certificado*, *LCR*

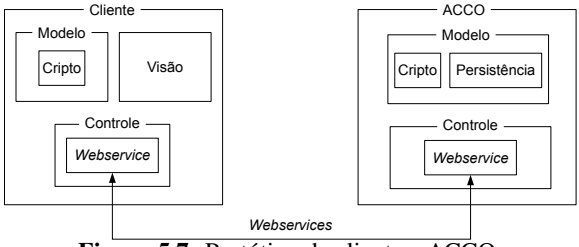

Figura 5.7: Protótipo de cliente e ACCO.

e *Carimbo do Tempo* relativas ao signatário. Em seguida, incluem-se no campo *certificados* de *PKCS#7* o CO e o certificado da ACCO. Por fim, modificam-se os campos *númeroSerial* e *nomeEmissor* de *IdSignatário* de acordo com os campos X.509 (Página 19) *Serial Number* e *Issuer* do CO, respectivamente.

5.4 CLIENTE E SERVIDOR

Para implementar a otimização de documentos assinados foram desenvolvidos protótipos de aplicações cliente e servidor, como ilustrado na Figura 5.7. O primeiro consiste em um software Java para criação e verificação de assinaturas no formato PKCS#7. Adicionalmente, o cliente também realiza a otimização de documentos assinados, através do uso de COs, que são solicitados a uma ACCO (servidor).

O lado do cliente possui o módulo *Visão* (Figura 5.8) para interação como o usuário. Há o módulo *Modelo* que, junto com o módulo *Cripto*, é responsável pelas operações criptográficas sobre documentos eletrônicos: assinar, verificar e otimizar. Por último, o cliente conta com os módulos *Controle* e *Webservices*, ambos responsáveis pelo comunicação via *webservices* com uma ACCO.

Análogo ao cliente, o software servidor para gerir uma ACCO foi desenvolvido em Java e também possui os módulos *Modelo* e *Controle* para as funcionalidades criptográficas e de comunicação. Todavia, esta parte do protótipo não possui interface gráfica (módulo *Visão*), dado que sua interação com clientes ocorre apenas por meio de *webservices*. Adicionalmente, o servidor possui o módulo *Persistência*, útil para registrar informações necessárias para emissão de COs, como carimbo do tempo relativo e número serial do último CO.

O fluxograma do processo de otimização de um documento eletrônico assinado é apresentado na Figura 5.9. Em 1, o cliente remove do PKCS#7 o conteúdo assinado, sobre o qual é calculado o resumo criptográfico (em 2). Isto é necessário para reduzir os custos de comunicação no passo seguinte. Em 3, solicita-se um CO, submetendo-se o PKCS#7 e resumo criptográfico. Em 3.1 a ACCO verifica a assinatura digital sobre o documento eletrônico e o certificado do signatário. Caso ambas as

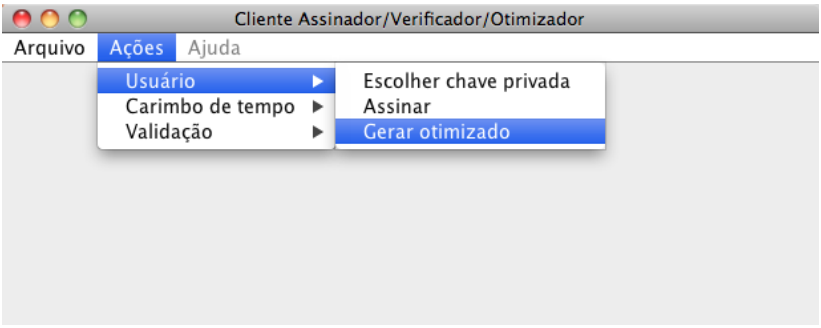

Figura 5.8: Interface gráfica cliente.

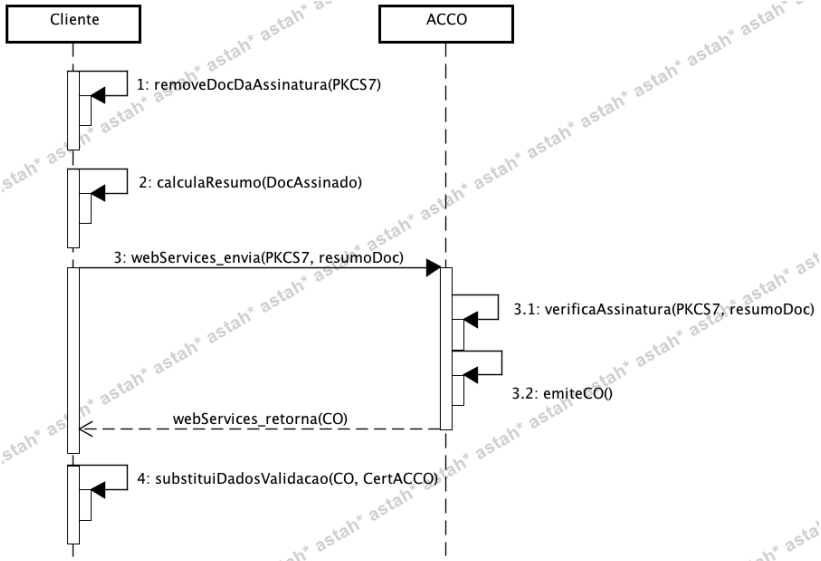

Figura 5.9: Diagrama de sequência da otimização de um documento eletrônico assinado.

verificações ocorram com sucesso, a ACCO emite um CO em 3.2, o qual é enviado ao cliente. Por fim, o cliente substitui os dados de validação pelo CO e o certificado da ACCO, como descrito na Seção 5.3.

5.5 *CRYPTO TIME*

Para dar suporte a gestão dos dados do Novomodo em uma ICPO criou-se um protótipo de aplicação para o *Crypto Time*. Esse aplicativo foi desenvolvido em PHP5 [81] e permite cadastrar e consultar dados do Novomodo para diferentes certificados. O objetivo principal da aplicação

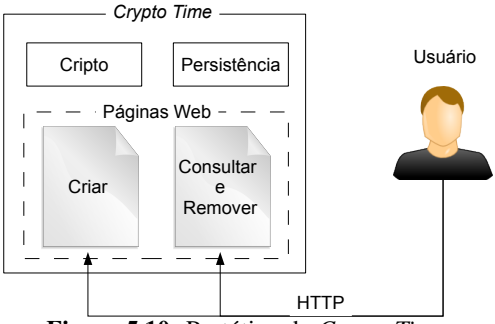

Figura 5.10: Protótipo do *Crypto Time*.

é facilitar a obtenção das informações de revogação em uma data arbitrária sem que o usuário precise realizar diversas operações aritméticas e de resumo criptográfico necessárias no método Novomodo.

Entretanto, optou-se por não implementar os requisitos de sigilo dos dados do Novomodo citados na Seção 4.4. Portanto, um usuário pode consultar todos os dados do Novomodo cadastrados. Essa decisão buscou simplificar o desenvolvimento do protótipo, tendo em vista que tal requisito de segurança não interfere nos testes de funcionamento da certificação otimizada.

A Figura 5.10 ilustra o protótipo do *Crypto Time*. Esse consiste de um cadastro de dados do Novomodo, implementado através do módulo *Persistência*. Essas informações são disponibilizadas a todos usuários através de duas páginas web (*Criar* e *Consultar e Remover*), acessíveis através do protocolo *Hypertext Transfer Protocol* (HTTP) especificado em [82].

Para criar novos dados do Novomodo para um certificado acessa-se a página *Criar* (Figura 5.11). Nesta há um formulário com os seguintes campos a serem preenchidos:

Issuer : nome do emissor do certificado (e.g. AC Raiz);

Serial : serial do certificado (e.g. 2);

Data de emissão : data no formato *Generalized Time* (fuso horário +0) de início do prazo de validade do certificado (e.g. 20100708150000Z);

Data de expiração : data no formato *Generalized Time* (fuso horário +0) de fim do prazo de validade do certificado (e.g. 2011708150000Z);

Granularidade : intervalo de tempo (em segundos) entre duas publicações de situação de revogação consecutivas (e.g. 86400).

Ao submeter o formulário da página *Criar* o módulo *Crypto* é acionado. Nele há um gerador de números aleatórios que gera os valores

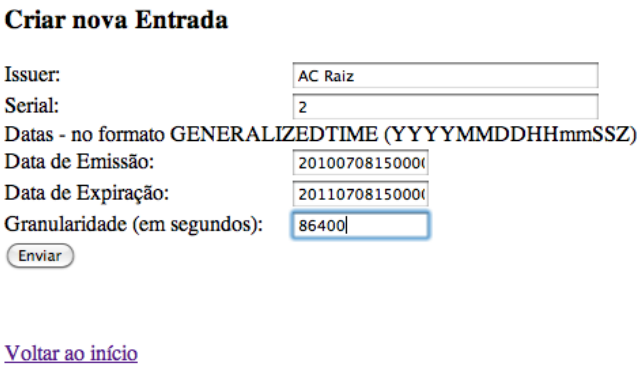

Figura 5.11: Página web para cadastrar novos dados do Novomodo.

secretos X_0 e Y_0 do método Novomodo. Estes dados, juntamente com as informações do formulário, são armazenados pelo módulo *Persistência*.

A página *Consultar e Remover* (Figura 5.12) permite visualizar e apagar os dados do Novomodo referentes a um certificado arbitrário. No topo da página há uma lista de certificados, que são identificados pelo números serial e nome do emissor. Selecionado o certificado, pode-se excluí-lo – através do botão *Apagar* – ou consultar os dados do Novomodo com base na data atual pressionando o botão *Consultar*. Para consultas usando outras datas, utiliza-se o campo de texto abaixo da lista de certificados, informando-se a data desejada no formato *Generalized Time* e pressionando o botão *Consultar*.

Ao pressionar o botão *Exibir* ou *Consultar* (Figura 5.12), o *Crypto Time* recupera do módulo *Persistência* o prazo de validade do certificado escolhido e os seguintes dados do Novomodo: granularidade (l), X_0 e Y_0. Em seguida, o *Crypto Time* calcula: a) o total (n) de situações de revogação (Equação 5.1) considerando-se as datas de início e fim do prazo de validade do certificado formatadas em *POSIX Time*[2]; b) o número (k) da situação de revogação referente a data desejada pelo usuário (Equação 5.2); c) X_{n-k} e Y_1, conforme apresentado na Seção 3.6.1. Por fim, o *Crypto Time* exibe as informações recuperadas do cadastro bem como aquelas calculadas.

$$n = \frac{fim - inicio}{granularidade} \tag{5.1}$$

$$k = \lfloor \frac{data - inicio}{granularidade} \rfloor \tag{5.2}$$

[2]Representação de datas padronizada ISO [83] em que se conta o número de segundos passados desde 01/01/1970 até uma data arbitrária.

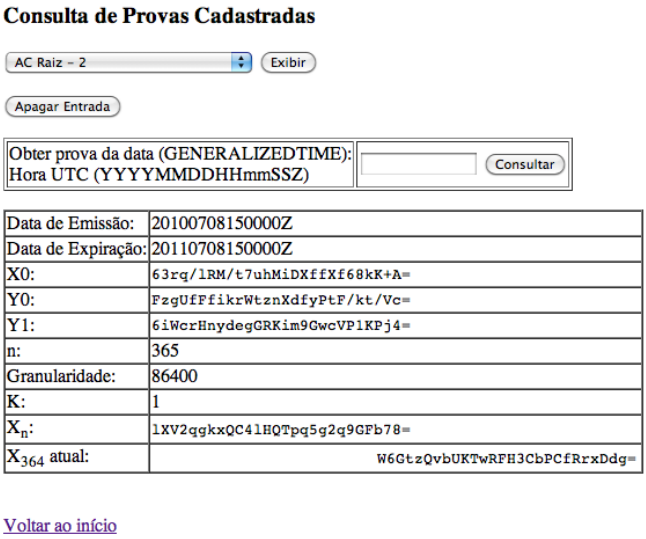

Figura 5.12: Página web para consultar e remover dados do Novomodo.

6 ANÁLISE

6.1 INTRODUÇÃO

Como mencionado anteriormente, o objetivo da Infraestrutura de Chaves Públicas Otimizadora é dar suporte a otimização de documentos eletrônicos assinados, reduzindo o esforço computacional para a verificação e manutenção a longo prazo de assinaturas digitais. De forma ao leitor compreender essa redução bem como as dificuldades para o emprego do Certificado Otimizado, este capítulo apresenta uma análise sobre a certificação otimizada.

Esta análise corresponde a uma compilação dos resultados observados nos testes sobre os protótipos (Capítulo 5) e em simulações de esforço computacional. Adicionalmente, complementou-se a análise com discussões realizadas entre os membros do LabSEC e críticas recebidas nas publicações deste trabalho ([19, 20]).

O restante deste Capítulo é organizado da seguinte forma. A Seção 6.2 analisa o CO sobre o ponto de vista de um artefato auto-verificável. A Seção 6.3 apresenta o processo de verificação da assinatura digital a partir de dados de validação otimizados. A Seção 6.4 aborda as restrições de uso do Certificado Otimizado em perfis de assinatura digital. Por fim, a Seção 6.5 propõe uma estimativa para os esforços computacionais de armazenamento e processamento, a qual é aplicada na simulação de um ambiente de certificação digital no âmbito da ICP-Brasil.

6.2 DOCUMENTOS ELETRÔNICOS ASSINADOS E AUTO-VERIFICÁVEIS

As primeiras propostas sobre o Certificado Otimizado [18, 19] apresentam o conceito de documentos eletrônicos assinados e auto-verificáveis. Trata-se de artefatos que contém todos os dados de validação necessários para verificar as assinaturas digitais e os certificados dos signatários. Por exemplo, estão encapsulados no documento assinado auto-verificável o Certificado Otimizado, o certificado da ACCO e os dados do Novomodo. Portanto, esse tipo de documento não exige a atualização dos dados de validação (e.g. a última situação de revogação), podendo assim ser mantido e verificado em ambientes computacionais isolados.

Idealmente, as propriedades do Certificado Otimizado seriam suficientes para a concepção de um documento assinado auto-verificável. Por exemplo, seria desnecessária a atualização das informações de revogação do caminho de certificação do CO, dado que aquele é válido por um instante particular de tempo (i.e. a data de emissão do CO). Adicionalmente, uma vez que o *Crypto Time* revoga a ACCO, um adversário não

teria condições de emitir COs falsos. Isto porque não é possível forjar a prova atual de validade do Novomodo (X_{n-k}) a partir da prova anterior (X_{n-k+1}), dada a dificuldade de se inverter uma função de resumo criptográfico F em $X_{n-k} = F^{-1}X_{n-k+1}$.

Contudo, verificou-se que é possível um adversário retroceder o relógio interno da ACCO e, em seguida, emitir COs cuja data de emissão remete ao passado. Para estes COs falsos o adversário utilizaria as provas de validade (X_{n-k}) publicadas anteriormente pelo *Crypto Time*. Desta forma, verificadores de documentos eletrônicos assinados e otimizados não perceberiam a fraude, pois não utilizariam a última situação de revogação e validariam o caminho de certificação do CO em uma data passada quando o ACCO ainda não havia sido comprometida.

Portanto, concluiu-se e se publicou em [20] que um documento eletrônico assinado e otimizado através do uso do CO não deve ser utilizado como um artefato auto-verificável quando o comprometimento da ACCO for possível. Neste caso, sugere-se que o verificador consulte sempre a última situação de revogação sobre a ACCO. Por outro lado, em ambientes em que o comprometimento da ACCO não fosse possível, poder-se-ia utilizar o CO como artefato auto-verificável. Nesta situação seriam dispensadas as provas de revogação (Y_0) e a cessão das provas de validade (X_{n-k}) causaria o bloqueio automático das operações da ACCO.

6.3 VERIFICAÇÃO DA ASSINATURA DO DOCUMENTO ELETRÔNICO

Através dos testes realizados sobre os protótipo de aplicação cliente (Seção 5.4), verificou-se que o caminho de certificação do CO foi verificado com sucesso pela a implementação do algoritmo *Certificate Path Processing* presente na Máquina Virtual Java (MVJ). Portanto, não houve problemas quanto ao CO ser válido por um instante particular de tempo.

Contudo, os provedores de serviços criptográficos presentes na MVJ e no *Bouncy Castle* não provêem suporte ao método de Novomodo. Todavia, esse esquema de revogação pode ser facilmente incorporado à plataforma Java sem interferir no *Certificate Path Processing*.

Verificou-se também que o protótipo de aplicação cliente foi capaz de validar, através da chave pública presente no CO, a assinatura digital sobre o documento eletrônico. Entretanto, esta operação poderia ser simplificada caso a ACCO fosse adaptada para a verificar também a assinatura sobre o documento eletrônico antes de emitir o CO. Portanto, nesta nova configuração, o CO atestaria a validade tanto da assinatura digital sobre o documento eletrônico quanto do caminho de certificação do signatário. Desta maneira, para verificar um documento eletrônico assinado o verificador deveria: a) confirmar se o resumo criptográfico da assinatura digital sobre o documento eletrônico equivale ao valor embarcado no CO; e b) verificar o caminho de certificação otimizado.

Por fim, embora seja possível alcançar uma economia extra de esforço de processamento, preferiu-se não simplificar a validação da assinatura sobre o documento eletrônico otimizado. Desse modo, a proposta de certificação otimizada presente neste trabalho mantém compatibilidade com as aplicações existentes de assinatura digital.

6.4 RESTRIÇÕES DE FORMATOS DE ASSINATURA DIGITAL

A otimização de um documento eletrônico assinado consiste em reduzir os dados de validação. Para tal, substituem-se artefatos, como o certificado do signatário pelo CO. Todavia, essa troca de certificados pode ser utilizada para outros fins, como ataques de substituição. Por exemplo, um signatário mal intencionado pode evitar que sua assinatura digital sobre um documento eletrônico seja validada. Para tal, ele troca seu certificado encapsulado no documento eletrônico assinado por outro certificado de mesma chave pública, porém revogado. Desta maneira, os verificadores não conseguem validar a assinatura digital nem perceber que o ataque de substituição ocorreu.

Sabe-se, entretanto, que os ataques de substituição são possíveis nos formatos de assinatura digital mais antigo, e.g. PKCS#7 e XMLdSig. Buscando corrigir essa vulnerabilidade, os novos formatos de assinatura digital (e.g. CMS, CAdES e XAdES) implementam a propriedade *ESS signing-certificate*, definida por [84]. Essa permite que o verificador perceba o ataque de substituição, dado que ela contém o resumo criptográfico do certificado que o signatário utilizou durante a criação da assinatura digital.

Portanto, conclui-se que tal propriedade presente nos formatos de assinatura digital avançados restringe a otimização de documentos eletrônicos assinados. Desse modo, resta a possibilidade de se utilizar o CO em formatos mais simples, como o PKCS#7 e XMLdSig.

6.5 REDUÇÃO DO ESFORÇO COMPUTACIONAL

Como apresentando anteriormente, a certificação otimizada permite simplificar a verificação e a manutenção a longo prazo das assinaturas digitais sobre documentos eletrônicos. Para compreender tal simplificação, comparam-se os esforços computacionais necessários para o uso de certificado convencionais e otimizados. Em seguida, apresenta-se uma simulação de uso de documentos eletrônicos assinados ao longo dos anos a fim de ilustrar as diferenças entre as duas abordagens de certificação digital descritas neste trabalho.

Primeiramente, sabe-se que, para se garantir a irretratabilidade de uma assinatura digital sobre um documento eletrônico, precisa-se construir e validar do caminho de certificação do signatário. A construção exige a descoberta e localização dos dados de validação, processo que exige esforço de comunicação, e.g. para acessar um repositório na rede.

Todavia, esse esforço pode ser reduzido se os dados de validação estiverem presentes no documento eletrônico assinado, porém, em contrapartida, se requer mais esforço de armazenamento. Ainda, vale lembrar que este esforço pode ser expressivamente incrementado caso haja LCRs longas.

Para ilustrar a relação inversa entre os esforços de armazenamento e comunicação apresenta-se a Figura 6.1. Esta ilustra a quantidade de dados de validação para uma assinatura digital no formato CAdES, considerando diferentes perfis e ignorando a restrição ao uso do Certificado Otimizado mencionada na Seção 6.4. Os valores apresentados podem ser obtidos através da simples contagem de artefatos presentes nas figuras da Seção 3.4, considerando que os caminhos de certificação possuem 3 certificados e ignorando a assinatura digital sobre o documento eletrônico.

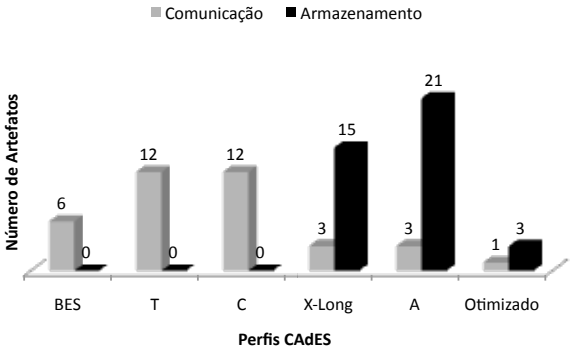

Figura 6.1: Relação entre esforços de comunicação e armazenamento em diferentes perfis de assinatura digital CAdES.

Na Figura 6.1 vê-se que no BES não há esforço de armazenamento, pois este perfil não incorpora dados de validação. Por outro lado, a validação de uma assinatura digital BES requer que o verificador obtenha, por consultas externas, 6 artefatos referentes ao caminho de certificação do signatário: 3 certificados e 3 artefatos de situação de revogação, totalizando 6 artefatos. Semelhante ao BES, estão os perfis T e C. Porém estes exigem que o verificador obtenha 6 artefatos adicionais, referente aos dados de validação do carimbo do tempo sobre a assinatura digital. Diferente desses perfis, está o X Long. Este encapsula os artefatos dos perfis anteriores (12) e, opcionalmente, os certificados (3) da Autoridade de Carimbo do Tempo (ACT) que emitiu o carimbo do tempo sobre o perfil C, totalizando 15 artefatos. Contudo, para verificar a situação de revogação da ACT são necessários obter 3 artefatos, representados como esforço de comunicação na Figura 6.1. Ainda, há o perfil A, que incorpora os dados de validação do perfil X Long e do carimbo do tempo de arquivamento. Para a validação de ACT também se exige um esforço de

comunicação estimado em 3 artefatos de situação de revogação.

Dentre os valores apresentados na Figura 6.1 destacam-se aqueles referentes ao perfil otimizado. Enquanto nos perfis BES, T, C, X Long e A são necessários obter no mínimo 3 artefatos por meio de consultas externas, no perfil Otimizado busca-se apenas 1 artefato: a prova de validade Novomodo (X_{n-k}). Não obstante, lembra-se que este artefato tem tamanho desprezível (e.g. 20 bytes) se comparado a certificados digitais e LCRs, fato que deve ser considerado durante uma transferência pela rede. Adicionalmente, X_{n-k} pode ser ignorado, como discutido na Seção 6.2. Ainda, percebe-se que o perfil otimizado se diferencia dos demais aos apresentar o menor esforço de armazenamento (3) referente aos seguintes artefatos: CO, certificado da ACCO e X_{n-k}, sendo o último de tamanho desprezível (e.g. 20 bytes).

Ao contrário do esforço de comunicação, que mantém-se constante e dependente do perfil de assinatura, os esforços de armazenamento e processamento crescem ao longo dos anos. Esse aumento tem sua causa na manutenção a longo prazo da autenticidade da assinatura digital (Capítulo 3), processo que faz uso de carimbos do tempo, aumentando a quantidade de dados de validação. Para ilustrar a evolução dos esforços computacionais apresenta-se a Figura 6.2.

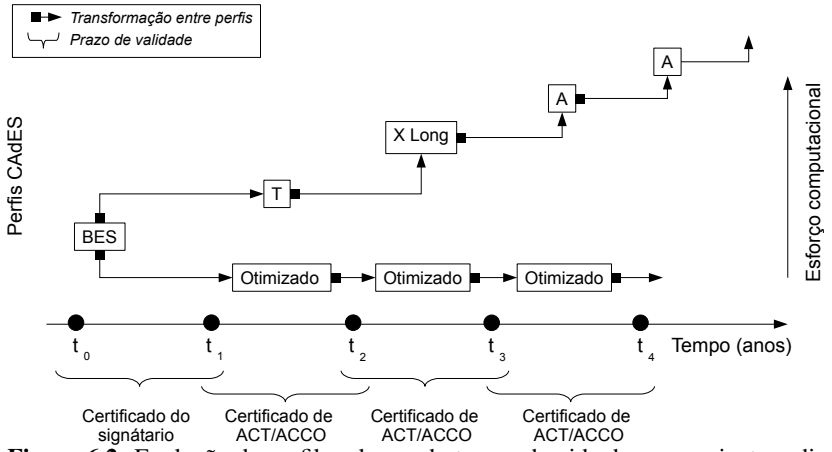

Figura 6.2: Evolução de perfil ao longo do tempo de vida de uma assinatura digital CAdES.

Na Figura 6.2 o eixo horizontal representa o tempo, medido em anos. Esse é segmentado pelos instantes t_0 a t_4, que representam os momentos em que ocorre a manutenção da autenticidade da assinatura, seja pela troca de certificado otimizado ou pela adição de um carimbo do tempo e, opcionalmente, a mudança de perfil de assinatura digital. Este processo é combinado com os prazos de validade do certificado de signatário, de ACCO ou de ACT. Tais períodos de tempo são representados

por chaves paralelas ao eixo horizontal. Ainda, os perfis de assinatura digital são posicionados verticalmente no gráfico de acordo com o esforço computacional que exigem do verificador de assinatura digital.

Portanto, vê-se na Figura 6.2 que uma assinatura básica no perfil BES é criada em t_0. Próximo ao fim do prazo de validade do certificado do signatário (t_1) adiciona-se um carimbo do tempo sobre a assinatura, evitando-se que esta deixe de ser válida. Assim, muda-se para o perfil T, com o objetivo para dar suporte a inclusão do carimbo. Em t_2, antes que expire o certificado da ACT que emitiu o carimbo, adiciona-se um carimbo do tempo sobre as referências e sobre o carimbo do tempo sobre a assinatura, evitando que o este último e, consequentemente, a assinatura do documento eletrônico, tornem-se inválidos. Dado que o perfil T não prevê o novo carimbo do tempo, migra-se para o perfil X Long, o qual inclui também os caminhos de certificação e LCRs do signatário e da ACT que emitiu o primeiro carimbo. Em t_3, antes que expire o certificado da ACT que emitiu o último carimbo, muda-se para o perfil A, incluindo os dados de validação da última ACT e adicionando um carimbo do tempo de arquivamento. A partir deste ponto o perfil permanece inalterado e novos carimbos do tempo de arquivamento podem ser empregados para contingenciar o enfraquecimento de algoritmos criptográficos utilizados ou a expiração do certificado de uma ACT.

Percebe-se que a dinâmica ilustrada causa o aumento do esforço computacional para validar e armazenar documentos eletrônicos assinados. Porém, pode-se, alternativamente, utilizar o perfil otimizado de assinatura em t_1, cujo esforço computacional é reduzido e constante ao longo dos anos. Isso ocorre pois não se acrescentam carimbos do tempo para tratar a expiração de certificados e o envelhecimento de algoritmos criptográficos. Faz-se, entretanto, a substituição de COs antigos, empregando-se novos caminhos de certificação otimizados.

Compreendida a dificuldade para se usarem documentos eletrônicos assinados, propõem-se agora equações para estimar os esforços de armazenamento (E_a) de processamento (E_p). Para o primeiro há a Tabela 6.1 e para o segundo a Tabela 6.2. Na Tabela 6.3 têm-se a descrição das variáveis envolvidas nas equações.

Tabela 6.1: Equações para cálculo do esforço de armazenamento.

Perfil CAdES	Equação
BES	$E_a = Doc + Sig$
T	$E_a = Doc + Sig + t$
X Long	$E_a = Doc + Sig + 2 \times t + 2 \times L \times (C + R)$
A	$E_a = Doc + Sig + (2 + n) \times t + (3 + n - 1) \times L \times (C + R)$
Otimizado	$E_a = Doc + Sig + 2 \times C + F + X_n + X_{n-k} + l + n$

Para calcular o valor de E_a referente ao BES – perfil que não prevê

encapsulamento de dados de validação – calcula-se o total de bytes necessários para armazenar um documento eletrônico (Doc) e a respectiva assinatura digital (Sig). Para o perfil T considera-se o valor de E_a para o perfil BES acrescido do carimbo do tempo sobre a assinatura (t). Para o perfil X Long tem-se o E_a referente ao T somado a: a) carimbo do tempo sobre as referências (t); e b) os certificados e LCRs dos caminhos de certificação do signatário e da ACT que emitiu o primeiro carimbo ($2 \times L \times (C + R)$). Para o perfil A adicionam-se ao E_a do X Long: a) n carimbos de arquivamento; b) os caminhos de certificação das ACTs que emitiram o carimbo do X Long e os n carimbos de arquivamento, com exceção do último. Por último, no perfil Otimizado contabilizam-se Doc, Sig, os certificados otimizado e da ACCO ($2 \times C$) e, por fim, os dados do Novomodo: F, X_n, X_{n-k}, l, p. Vale lembrar que, com exceção de X_{n-k}, os demais dados do Novomodo são encapsulados pela ACCO nos COs, por este motivo não foram considerados na Figura 6.1.

Tabela 6.2: Equações para cálculo do esforço de processamento.

Perfil CAdES	Equação
BES	$E_p = 1 + 2 \times L$
T	$E_p = 2 + 4 \times L$
X Long	$E_p = 3 + 6 \times L$
A	$E_p = 3 + n + 2 \times L \times (3 + n)$
Otimizado	$E_p = 3$

Tabela 6.3: Variáveis para estimar esforços computacionais.

Variável	Descrição
Doc	Documento eletrônico assinado
C	Certificado digital
L	Comprimento de caminho de certificação
R	LCR
t	Carimbo do tempo
n	Quantidade de carimbos do tempo de arquivamento
Sig	Assinatura digital
F	Identificador de função de resumo criptográfico
X_{n-k}	Prova de validade
X_n	Alvo de validade
l	Tempo para revogação
p	Total de provas

Referente aos perfis X Long e A, é interessante comentar que geralmente não se embarcam em um documento eletrônico assinado os certificados e LCRs do caminho de certificação do último carimbo do tempo afixado. Embora seja possível embarcar os certificados, este trabalho en-

tende que as LCRs não devem ser encapsuladas, dado que suas cópias mais recentes devem ser consultadas no momento da verificação do documento eletrônico assinado, garantindo assim que a chave privada da ACT não tenha sido comprometida.

Não obstante, Denis Pinkas em [85] destaca a baixa probabilidade de que a chave privada de uma ACT venha a ser comprometida, haja vista os rígidos requisitos de segurança a serem contemplados por uma ACT. Caso se aceite essa premissa como verdadeira, podem-se encapsular as LCRs bem como validar o caminho de certificação da ACT com base na data de emissão do carimbo do tempo. Sem dúvida, tal decisão reduziria consideravelmente o esforço computacional, dado que se desprezaria a expiração do certificado da ACT e a adição de novos carimbos do tempo de arquivamento ocorreria poucas vezes ao longo da vida de um documento eletrônico. Isso porque tais artefatos seriam utilizados apenas para contingenciar o enfraquecimento dos algoritmos criptográficos, o qual é um processo normalmente lento.

Para calcular o valor de E_p deve-se contabilizar a quantidade de artefatos assinados, cujas assinaturas devem ser validadas durante a verificação do documento eletrônico assinado. Portanto, cálculo de E_p para o perfil BES considera: a assinatura sobre Doc (1) e os certificados e as LCRs presentes do caminho de certificação do signatário ($2 \times L$). Para o perfil T, considera-se o valor de E_p para o BES acrescido do carimbo do tempo sobre a assinatura (1) e dos certificados e as LCRs presentes no caminho de certificação da ACT ($2 \times L$). Para o perfil X Long, considera-se o valor de E_p para o T acrescido do carimbo do tempo sobre as referências (1) e os certificados e as LCRs do caminho de certificação da ACT emissora ($2 \times L$). Para o perfil A, considera-se o valor de E_p para o X Long acrescido de n carimbos de arquivamento e os certificados e as LCRs dos caminhos de certificação das n ACTs emissoras.

Diferente dos outros perfis, o Otimizado apresenta um valor fixo para E_p, como ilustra a Tabela 6.2. A constante 3 equivale ao total de assinaturas digitais sobre os seguintes artefatos: o conteúdo assinado (Doc), o CO e o certificado da ACCO. Embora presente na verificação dos artefatos, opta-se por desconsiderar o método Novomodo no cálculo de E_p. A justificativa está no esforço computacional inerente a funções de resumo criptográfico, que é desprezível se comparado ao das operações de criptografia assimétrica, cuja complexidade é maior em diversas ordens de grandeza [86].

Por fim, a simples análise dos gráficos e das equações permite ao leitor perceber a diferença entre os perfis CAdES apresentados. A fim subsidiar essa comparação com valores próximos da realidade, apresenta-se a simulação a seguir.

Tabela 6.4: Cronograma para evolução de perfil de assinatura utilizando certificação digital convencional.

Perfil CAdES	Ano								
	1	2	3	4	5	6	7	8	≥ 9
BES	●	●	○						
T			●	●	○				
X Long					●	●	○		
A							●	●	●
Otimizado			●	●	●	●	●	●	●

6.5.1 Simulação

Para ilustrar a evolução do esforço de computacional, apresenta-se o seguinte cenário. Um usuário final, titular de um certificado digital ICP-Brasil A3 [74] cujo par de chaves mede 1024 bits, assina um documento eletrônico que mede 750kB. A assinatura digital segue o perfil CAdES-BES e é mantida válida por 100 anos através de duas abordagens: adição de carimbos tempo – emitidos por ACTs titulares de certificados T4 [74] – ou uso de Certificado Otimizado.

Haja vista que certificados A3, T4 e otimizados têm validade de 3 anos, estipula-se o cronograma apresentado na Tabela 6.4 para as modificações de perfil da assinatura digital sobre o documento eletrônico. Marcam-se com o símbolo (●) os anos em que um perfil permanece inalterado. Já nos anos sinalizados com o símbolo (○) muda-se o perfil de assinatura digital. Tal mudança pode ocorrer a qualquer dia do ano destacado por (○), sendo o melhor caso quando ela ocorre no último dia daquele ano.

Portanto, vê-se na Tabela 6.4 que o usuário cria uma assinatura CAdES cujo perfil é BES. Antes do fim do terceiro ano têm-se duas opções para a manutenção da autenticidade da assinatura digital: a) a migração para o perfil T, incluindo-se um carimbo do tempo sobre a assinatura; ou b) a otimização dos dados de validação, migrando-se para o perfil Otimizado. Caso se opte por a), a mudança entre perfis ocorre até o sétimo ano. Nos anos seguintes mantém-se o perfil A e incluem-se carimbos do tempo de arquivamento a cada 3 anos. Por outro lado, se escolhida a opção b), o perfil Otimizado permanece ao longo dos anos, sendo necessário somente a troca de Certificado Otimizado a cada 3 anos.

Com base no cronograma apresentado calculam-se os esforços de armazenamento (E_a) e de processamento (E_p) considerando, respectivamente, as equações das tabelas 6.1 e 6.2. Adicionalmente, Tabela 6.5 apresenta valores para as variáveis das equações. Esses foram obtidos por membros do LabSEC através de amostras de artefatos presentes em repositórios da ICP-Brasil e por meio do uso dos protótipos desenvolvidos (Capítulo 5).

Calculados os valores de E_a apresenta-se a Figura 6.3 . Dentre os valores ilustrados, destaca-se o armazenamento dos dados de validação

Tabela 6.5: Valores para estimar esforços computacionais.

Variável	Descrição	Valor Médio (kB)
Doc	Documento eletrônico assinado	750
C	Certificado X.509	1,1
Sig	Assinatura digital	0,125
F	Identificador de função de resumo criptográfico	0,07
X_{n-k}	Prova de validade	0,02
X_n	Alvo de validade	0,02
l	Tempo para revogação	0,04
p	Total de provas	0,04

convencionais, resultado da adição de carimbos do tempo. Vê-se que, inicialmente, tais valores são desprezíveis se comparados ao documento eletrônico assinado. Entretanto, a partir do 5º ano utilizam-se os perfis X Long e A, que incorporam os dados de validação: carimbos do tempo, cadeias de certificados e situações de revogação do signatário e ACTs. Tal inclusão causa o aumento expressivo dos dados de validação convencionais que, após 25, 50 e 100 anos, representam, respectivamente, 68,8%, 81,5% e 90,1% de E_a.

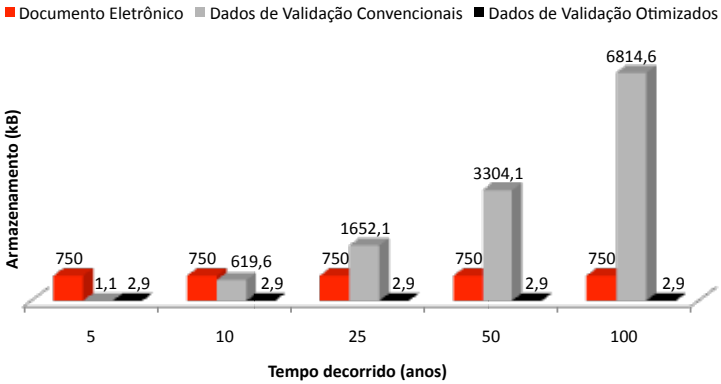

Figura 6.3: Evolução do esforço de armazenamento ao longo de 100 anos nas abordagens convencional e otimizada de certificação digital.

Por outro lado, o uso do perfil Otimizado mostra-se vantajoso frente à adição de carimbos do tempo. Nota-se que o armazenamento dos dados de validação otimizados é constante ao longo dos anos e representa somente 0,4% de E_a. Deste modo, o emprego de Certificado Otimizado proporcionaria uma redução de quase 100% do volume de dados de validação frente a abordagem convencional. Não obstante, o leitor

pode questionar que o perfil Otimizado é desvantajoso nos 5 primeiros anos. De fato, os perfis BES e T vigentes nesse período exigem menos bytes, mas apresentam E_p alto em contra-partida. Este trabalho busca não priorizar um tipo de esforço computacional, portanto se opta por incluir o mínimo de dados de validação de modo a se obterem valores reduzidos para E_a e E_p.

Os valores obtidos para E_p são ilustrados na Figura 6.4. Vê-se que o número de assinaturas digitais sobre os dados de validação convencionais contrastam com a única assinatura sobre o documento eletrônico. Isto ocorre porque a adição de um carimbo do tempo a cada 3 anos incorpora 7 novos artefatos assinados: 1 carimbo do tempo, 3 certificados digitais e 3 situações de revogação referentes ao caminho de certificação de ACT. Nesta dinâmica, inicialmente os dados de validação convencionais representam 92,9% de E_p, chegando a 99,6% no final do tempo de vida da assinatura digital.

Novamente, a certificação digital otimizada apresenta-se como a abordagem mais vantajosa desta simulação. Na Figura 6.4 nota-se que o número de assinatura digitais sobre os dados de validação otimizados é constante ao longo dos anos, representando 66,67% de E_p. Ainda, na troca de dados de validação convencionais por otimizados o processamento de assinaturas seria reduzido em: 84,6% após o 5º ano; 94,1% após o 10º ano; 96,7% após o 25º ano; 98,3% após 50º ano; e 99,2% após 100º ano.

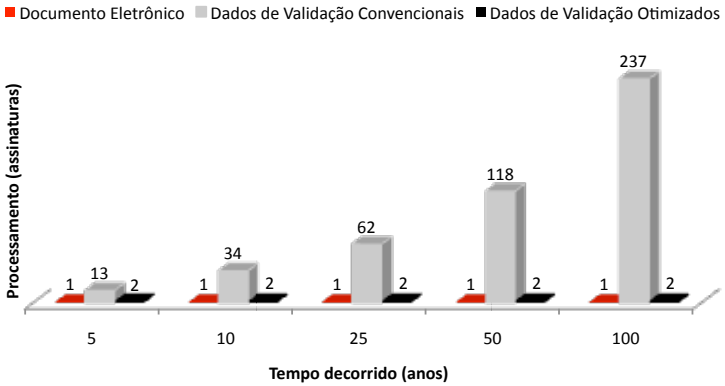

Figura 6.4: Evolução do esforço de processamento ao longo de 100 anos nas abordagens convencional e otimizada de certificação digital.

Por fim, através das figuras 6.3 e 6.4 pode-se concluir que a redução de esforço computacional alcançada é expressiva para um ambiente de certificação digital de documentos eletrônicos similar a ICP-Brasil. Não obstante, sabe-se que a escolha de diferentes valores para as variáveis utilizadas (Tabela 6.5) pode mudar consideravelmente o resultado da

simulação, em especial as estimativas de armazenamento (E_a). Por exemplo, a redução do tamanho da LCR (67,4 kB) levaria a diferentes resultados. Porém, vale lembrar que há registros, inclusive na ICP-Brasil, de LCRs cujos tamanhos são superiores ao utilizado aqui.

6.6 CONCLUSÃO

Este capítulo apresentou uma análise sobre o uso de Certificados Otimizados, destacando restrições e benefícios da certificação otimizada. As considerações descritas foram fundamentadas no uso dos protótipos desenvolvidos bem como nas contribuições da comunidade científica e dos membros do LabSEC.

Inicialmente, mostrou-se que um ambiente de certificação digital *offline*, em que não se atualiza a situação de revogação Novomodo, é suscetível a ataques. Por esse motivo, o CO não pode ser considerado um artefato assinado e auto-verificável.

Em seguida, abordou-se a compatibilidade do CO com as aplicações de certificação digital existentes. Viu-se que a assinatura digital sobre um documento eletrônico pode ser verificada pelo CO. Este, por sua vez, foi verificado com sucesso pela Máquina Virtual Java, porém sem considerar a situação de revogação Novomodo. Mostrou-se também que é possível realizar ajustes na certificação digital otimizada, reduzindo o esforço de processamento. Contudo, tal modificação comprometeria a compatibilidade do Certificado Otimizado. Ainda, apresentou-se a restrição ao uso do Certificado Otimizado em perfis avançados de assinatura digital (CAdES e XAdES), os quais inviabilizam a redução dos dados de validação.

Por fim, propôs-se uma estimativa para os esforços computacionais de armazenamento e de processamento. Essa proposta foi empregada na simulação de um ambiente de documentos eletrônicos assinados no âmbito da ICP-Brasil. Com base nos valores obtidos comprovou-se que a manutenção da autenticidade da assinatura digital por meio de carimbos do tempo incrementa linearmente o volume de dados de validação. Entretanto, estes podem ser minimizados e mantidos constantes através do CO – solução atraente para a economia de recursos computacionais.

7 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Este trabalho teve como objetivo apresentar uma solução para simplificar a verificação e a manutenção a longo prazo de assinaturas digitais sobre documentos eletrônicos. A técnica desenvolvida explora o conceito de uma entidade notarial *online* denominada Autoridade Certificadora de Certificados Otimizados, a qual emite um tipo especial de certificado: o Certificado Otimizado. Este opera como um atestado de validade do certificado digital do signatário. Além disso, um CO prestes a se tornar inválido pode ser facilmente substituído por outro, evitando o acúmulo de dados de validação que se observa nas técnicas convencionais. Por exemplo, aquelas baseadas na adição de carimbos do tempo.

Abordaram-se, no Capítulo 2, os conceitos sobre os quais se alicerça a certificação digital de documentos eletrônicos. Através dessa tecnologia atendem-se requisitos de segurança como autenticidade e integridade de conteúdos digitais. Adiante, o Capítulo 3 detalhou como avaliar a validade de assinaturas digitais sobre documentos eletrônicos. Viu-se que, diferente de assinaturas de próprio punho, as assinaturas digitais têm validade finita. Esta, todavia, pode ser prolongada através da adição de carimbos do tempo, processo denominado neste trabalho como *manutenção a longo prazo da autenticidade da assinatura digital*.

O Capítulo 3 dedicou-se também descrever formatos de assinatura digital, os quais dão suporte à inclusão de dados de validação – carimbos do tempo, certificados, LCRs. Mostrou-se, em seguida, que o crescimento dos dados de validação intensifica a dificuldade para verificar uma assinatura digital, fato que pode tornar proibitivo o uso de documentos eletrônicos assinados em ambientes com recursos computacionais escassos. Por fim, o capítulo apresentou soluções presentes na literatura que buscam facilitar o uso da certificação digital.

Nesse contexto, o Capítulo 4 apresentou a Infraestrutura de Chaves Públicas Otimizadora, cujo elemento fundamental é o Certificado Otimizado, emitido pela Autoridade Certificadora de Certificados Otimizados. Além destes conceitos, descreveram-se um mecanismo de revogação baseado no Novomodo e um sistema de registros para auditoria da emissão de Certificados Otimizados. Ao final do capítulo mostrou-se a aplicação das ideias apresentadas através do emprego de Certificados Otimizados dentro de um domínio de usuários que fazem uso de documentos assinados.

Para testar a certificação otimizada implementaram-se protótipos, os quais foram descritos no Capítulo 5. Nesta tarefa de desenvolvimento participaram alunos de graduação, que aplicaram conhecimentos sobre a linguagem Java, PHP e ASN.1. Os protótipos foram importantes para avaliar a aderência do Certificado Otimizado ao padrão X.509 e coletar informações para simulação e análise de esforço computacional.

A avaliação da conformidade do Certificado Otimizado segundo o X.509 foi positiva, pois a implementação do algoritmo *Certificate Path Processing* presente na Máquina Virtual Java foi capaz de validar o caminho de certificação otimizado. Com base nesse resultado, é de se esperar que as demais implementações deste algoritmo (e.g. Microsoft .NET [87] e OpenSSL [88]) comportem-se da mesma maneira, haja vista que as especificações técnicas do X.509 [11, 45] não mencionam restrições para a validade do certificado otimizado, i.e. *notBefore=notAfter*.

No Capítulo 6 apresentou-se uma análise do uso do Certificado Otimizado. Nesta apresenta-se a proposta de uma estimativa de esforços de armazenamento e de processamento para documentos eletrônicos assinados convencionais e otimizados. A comparação dos valores obtidos evidenciou uma economia superior a 80% dos recursos computacionais através da certificação otimizada. Com certeza, esta representa uma atraente solução à complexidade da verificação e manutenção a longo de assinaturas digitais sobre documentos eletrônicos.

Não obstante, ressalta-se que os benefícios da certificação otimizada contemplam apenas os verificadores de documentos assinados, e não os signatários. Todavia, lembra-se que o signatário verifica uma única vez a validade de seu certificado digital antes de assinar um documento eletrônico, enquanto verificadores podem utilizar o mesmo documento eletrônico assinado diversas vezes e, em todas, devem validar a assinatura e o certificado digitais do signatário.

Por outro lado, o leitor pode questionar a possibilidade de sobrecarga da ACCO perante inúmeras requisições de CO em um domínio. Porém, a otimização de documentos assinados é opcional na ICPO e pode ser efetuada a qualquer momento. Portanto, a sobrecarga da ACCO é de fato possível, mas uma política racional de emissão de CO, aliada a diversas instâncias de ACCOs, é totalmente concebível dentro da ICPO sem comprometer o uso de documentos eletrônicos assinados.

Este trabalho incentiva outros pesquisadores a buscarem soluções para tornar mais simples o uso dos serviços oferecidos pela Infraestrutura de Chaves Públicas. Na opinião do autor, os altos custos computacionais decorrentes da manutenção da autenticidade de uma assinatura digital é um problema que está vindo a tona, enquanto a sociedade se dá conta que deverá tratar um legado de documentos eletrônicos assinados em breve. Trabalhos como este ou que superem os COs serão de extrema utilidade a entidades arquivísticas, como por exemplo, tribunais, o Arquivo Nacional e notários.

Como sugestão de ponto de partida para trabalhos futuros sobre certificação otimizada tem-se a verificação da integridade e autenticidade da assinatura digital (Seção 6.3). Sugere-se que a ACCO verifique também a assinatura sobre documento eletrônico antes de emitir o CO. Mais tarde, o verificador da assinatura digital sobre o documento eletrônico otimizado não precisaria utilizar a chave pública do Certificado Otimizado, mas sim comparar o resumo criptográfico da assinatura digi-

tal com aquele encapsulado no CO (Figura 5.2), ganhando-se, assim, em performance. Entretanto, tal modificação deverá encontrar um meio de garantir a compatibilidade com as aplicações já existentes de certificação digital.

Sabe-se também que a utilização de CO é de fato limitada pelos formatos de assinaturas recentes, os quais impedem a substituição de certificados como citado na Seção 6.4. Trabalhos futuros podem tratar esta limitação por meio de outros artifícios, ficando como sugestão do autor explorar o uso de contra-assinaturas, através das quais serviços notariais poderiam atestar validade.

Por último, fica a possibilidade de se utilizar o CO de maneira auto-verificável, desde que se considere a impossibilidade da chave privada da ACCO ser comprometida. Uma vez que esta premissa é questionável na prática, dado que a ACCO é um serviço *online* exposto a adversários, sugere-se que trabalhos futuros desenvolvam artifícios que impeçam o reúso das provas Novomodo. Na opinião do autor, uma solução baseada em carimbos do tempo *offline* [89] poderia ser alcançada.

REFERÊNCIAS

[1] Estados Unidos. Uniform Electronic Transactions Act (UETA), 1999. Disponível em: <http://www.law.upenn.edu/bll/ulc/uecicta/uetast84.htm>. Acesso em 05/04/2010.

[2] Estados Unidos. Government Paperwork Elimination Act (GPEA), 2000. Disponível em: <http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html>. Acesso em 05/04/2010.

[3] TJ-SP. **Sai de cena o Diário Oficial em papel**. Disponível em: <http://www.tj.sp.gov.br/Noticias/NoticiasView.aspx?Id=143>. Acesso em: 01/07/2010.

[4] TJ-SP. **Workshop discute uso de documentos eletrônicos na Justiça**. Disponível em: <http://www.tj.sp.gov.br/Noticias/NoticiasView.aspx?Id=2126>. Acesso em: 01/07/2010.

[5] DIFFIE, W.; HELLMAN, M. E. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22, p. 644–654, 1976.

[6] KOHNFELDER, L. M. *Towards a practical public-key cryptosystem*. [S.l.], 1978.

[7] BERBECARU, D.; LIOY, A.; MARIAN, M. On the Complexity of Public-Key Certificate Validation. In: *ISC '01: Proceedings of the 4th International Conference on Information Security*. London, UK: [s.n.], 2001. p. 183–203. ISBN 3-540-42662-0.

[8] DZUNG, D. et al. Security for industrial communication systems. *Proceedings of the IEEE*, v. 93, n. 6, p. 1152–1177, June 2005. ISSN 0018-9219.

[9] SATIZáBAL, C. et al. Building a virtual hierarchy to simplify certification path discovery in mobile ad-hoc networks. *Comput. Commun.*, Butterworth-Heinemann, Newton, MA, USA, v. 30, n. 7, p. 1498–1512, 2007. ISSN 0140-3664.

[10] WILLIG, A. Recent and emerging topics in wireless industrial communications: A selection. *IEEE Transactions on Industrial Informatics*, v. 4, n. 2, p. 102–124, May 2008. ISSN 1551-3203.

[11] ITU-T. *Recommendation X.509 (08/2005) - Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*. [S.l.], 2005.

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

[13] MARTINEZ-PEL, R. et al. Efficient Certificate Path Validation and Its Application in Mobile Payment Protocols. *2008 Third International Conference on Availability, Reliability and Security*, IEEE, p. 701–708, mar. 2008.

[14] LEVI, A.; CAGLAYAN, M. U.; KOC, C. K. Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure. *ACM Trans. Inf. Syst. Secur.*, New York, NY, USA, v. 7, p. 21–59, 2004. ISSN 1094-9224.

[15] RIVEST, R. L. Can We Eliminate Certificate Revocations Lists? In: *FC '98: Proceedings of the Second International Conference on Financial Cryptography*. London, UK: [s.n.], 1998. p. 178–183. ISBN 3-540-64951-4.

[16] MICALI, S. NOVOMODO: Scalable Certificate Validation and Simplified PKI Management. In: *Proceedings of the 1st Annual PKI Research Workshop*. NIST, Gaithersburg MD, USA: [s.n.], 2002.

[17] GUTMAN, P. PKI: It's Not Dead, Just Resting. *Computer*, Los Alamitos, CA, USA, v. 35, p. 41–49, 2002. ISSN 0018-9162.

[18] NOTOYA, A. E. et al. Certificados Otimizados para a validação eficiente da Assinatura Digital. In: *IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*. Rio de Janeiro: [s.n.], 2007.

[19] CUSTóDIO, R. F. et al. Optimized Certificates - A New Proposal for Efficient Electronic Document Signature Validation. In: LSNES, S. F. M.; MAUW, S.; KATSIKAS, S. K. (Ed.). *EuroPKI*. [S.l.]: Springer, 2008. (Lecture Notes in Computer Science, v. 5057), p. 49–59. ISBN 978-3-540-69484-7.

[20] VIGIL, M. A. G. et al. Infra-estrutura de Chaves Públicas Otimizada: Uma ICP de Suporte a Assinaturas Eficientes para Documentos Eletrônicos. In: *IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*. Campinas: [s.n.], 2009.

[21] SCHöNROCK, K. A. *Desenvolvimento de aplicações provedoras de serviços criptográficos: carimbos de tempo e otimização de certificados*. Monografia (Bacharelado em Ciências da Computação) — Universidade Federal de Santa Catarina, 2009.

[22] BONDAN, L. S. d. C. G. I. R. *Autoridade Certificadora Otimizadora*. Monografia (Bacharelado em Ciências da Computação) — Universidade Federal de Santa Catarina, 2009.

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

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

[25] CALLAS, J. et al. *OpenPGP Message Format*. IETF, nov. 1998. RFC 2440 (Proposed Standard). (Request for Comments, 2440). Obsoleted by RFC 4880. Disponível em: <http://www.ietf.org/rfc/rfc2440.txt>.

[26] SCHMIDT, A. U.; LOEBL, Z. Legal Security for Transformations of Signed Documents: Fundamental Concepts. In: CHADWICK, D.; ZHAO, G. (Ed.). *EuroPKI 2005*. [S.l.: s.n.], 2005. (Lecture Notes in Computer Science, v. 3545), p. 255–270.

[27] MASINTER, L.; WELCH, M. A System for Long-Term Document Preservation. In: *IS&T Archiving 2006*. Ottawa, Canada: Society For Imaging Science And Technology, 2006. v. 3, p. 61–68.

[28] Eastlake 3rd, D.; JONES, P. *US Secure Hash Algorithm 1 (SHA1)*. IETF, set. 2001. RFC 3174 (Informational). (Request for Comments, 3174). Updated by RFC 4634. Disponível em: <http://www.ietf.org/rfc/rfc3174.txt>.

[29] MENEZES, A. J.; VANSTONE, S. A.; OORSCHOT, P. C. V. *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, Inc., 1996. ISBN 0849385237.

[30] SECURE Hash Standard. Washington: National Institute of Standards and Technology, 2004. Federal Information Processing Standard (FIPS) Publication 180-2. Disponível em: <http://csrc.nist.gov/publications/fips/>.

[31] DOBBERTIN, H.; BOSSELAERS, A.; PRENEEL, B. Ripemd-160: A strengthened version of ripemd. In: *Proceedings of the Third International Workshop on Fast Software Encryption*. London, UK: Springer-Verlag, 1996. p. 71–82. ISBN 3-540-60865-6.

[32] WANG, X. et al. Cryptanalysis of the hash functions md4 and ripemd. In: *EUROCRYPT*. [S.l.: s.n.], 2005. p. 1–18.

[33] YAJIMA, J. et al. A strict evaluation on the number of conditions for sha-1 collision search. *IEICE Transactions*, v. 92-A, n. 1, p. 87–95, 2009.

[34] AUMASSON, J.-P.; MEIER, W.; MENDEL, F. *Preimage Attacks on 3-Pass HAVAL and Step-Reduced MD5*. 2008. Cryptology ePrint Archive, Report 2008/183. `http://eprint.iacr.org/`.

[35] SASAKI, Y.; AOKI, K. Preimage attacks on step-reduced md5. In: *ACISP*. [S.l.: s.n.], 2008. p. 282–296.

[36] BURR, W. E. *NIST COMMENTS ON CRYPTANALYTIC ATTACKS ON SHA-1*. 2006. Disponível em: <http://csrc.nist.gov/groups/ST/hash/statement.html>.

[37] CLAEYS, S. J. *Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA–3) Family*. National Institute of Standards and Technology (NIST), 2007. 9 p. Disponível em: <http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf>.

[38] RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. M. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, v. 21, n. 2, p. 120–126, 1978.

[39] JOHNSON, D.; MENEZES, A.; VANSTONE, S. The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, Springer, v. 1, n. 1, p. 36–63, 2001.

[40] CHADWICK, D. W. *Understanding X.500 (The Directory)*. International Thompson Publishing, 1996. Disponível em: <http://www.cs.kent.ac.uk/pubs/1996/2051>.

[41] ITU-T. *Recommendation X.509 (11/88) - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*. 1988.

[42] ITU-T. *Recommendation X.509 (11/93) - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*. 1993.

[43] ITU-T. *Recommendation X.509 (11/2008) - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*. 2008.

[44] HOUSLEY, R.; POLK, T. *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*. New York, NY, USA: John Wiley & Sons, Inc., 2001. ISBN 0471397024.

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

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

[47] ITU-T. *Recommendation X.680 (11/2008) - Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[48] W3C. **Extensible Markup Language (XML)**. Disponível em: <http://www.w3.org/XML/>. Acesso em 06/07/2010.

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

[50] HOUSLEY, R. *Cryptographic Message Syntax (CMS)*. IETF, jul. 2004. RFC 3852 (Proposed Standard). (Request for Comments, 3852). Obsoleted by RFC 5652, updated by RFCs 4853, 5083. Disponível em: <http://www.ietf.org/rfc/rfc3852.txt>.

[51] Eastlake 3rd, D.; REAGLE, J.; SOLO, D. *(Extensible Markup Language) XML-Signature Syntax and Processing*. IETF, mar. 2002. RFC 3275 (Draft Standard). (Request for Comments, 3275). Disponível em: <http://www.ietf.org/rfc/rfc3275.txt>.

[52] ETSI. *PDF Advanced Electronic Signature Profiles;*: Part 1: PAdES overview – a framework document for PAdES. 1.1.1. ed. [S.l.], 2009.

[53] ETSI. *PDF Advanced Electronic Signature Profiles;*: Part 2: PAdES Basic – Profile based on ISO 32000-1. 1.2.1. ed. [S.l.], 2009.

[54] ETSI. *PDF Advanced Electronic Signature Profiles;*: Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles. 1.1.1. ed. [S.l.], 2009.

[55] ETSI. *XML Advanced Electronic Signatures (XAdES)*. [S.l.: s.n.], 2006.

[56] ETSI. *CMS Advanced Electronic Signatures (CAdES)*. [S.l.: s.n.], 2008.

[57] LLOYD, S.; OTHERS. Understanding certification path construction. In: *PKI forum white paper*. [S.l.: s.n.], 2002.

[58] MARTINEZ-PELáEZ, R. et al. Efficient certificate path validation and its application in mobile payment protocols. In: *ARES '08: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security*. Washington, DC, USA: IEEE Computer Society, 2008. p. 701–708. ISBN 978-0-7695-3102-1.

[59] GUIDA, R. et al. Deploying and using public key technology: lessons learned in real life. *IEEE Security and Privacy Magazine*, v. 2, n. 4, p. 67–71, jul. 2004. ISSN 1540-7993.

[60] AC SERASA SRF. **Lista de Certificados Revogados (LCR)**. Disponível em: <http://publicacao.certificadodigital.com.br/repositorio/lcr/SerasaSRF.crl>. Acesso em 24/02/2010.

[61] HALLAM-BAKER, P. *OCSP Extensions*. [S.l.]: IETF, 1999. Work in progress, IETF PKIX working group.

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

[63] ADAMS, C. et al. *Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols*. IETF, fev. 2001. RFC 3029 (Experimental). (Request for Comments, 3029). Disponível em: <http://www.ietf.org/rfc/rfc3029.txt>.

[64] RNES, A. A. et al. Selecting Revocation Solutions for PKI. In: *Proceedings of NORDSEC 2000 Fifth Nordic Workshop on Secure IT Systems*. Reykjavik: [s.n.], 2000.

[65] MICALI, S. *Enhanced Certificate Revocation System*. Cambridge, MA, USA, 1995.

[66] MCDANIEL, P.; JAMIN, S.; ARBOR, A. Windowed Key Revocation in Public Key Infrastructures. *IEEE INFOCOM*, v. 3, p. 1406–1414, 2000.

[67] COOPER, D. A. A model of certificate revocation. In: *ACSAC '99: Proceedings of the 15th Annual Computer Security Applications Conference*. Washington, DC, USA: IEEE Computer Society, 1999. p. 256. ISBN 0-7695-0346-2.

[68] PERLMAN, R.; KAUFMAN, C. *Method of Issuance and Revocation of Certificates of Authenticity Used in Public Key Networks and Other Systems*. [S.l.], 1993.

[69] ADAMS, C.; ZUCCHERATO, R. *A general, flexible approach to certificate revocation*. June 1998. Entrust Technologies White Paper.

[70] KOCHER, P. C. On certificate revocation and validation. *Financial Cryptography*, Springer-Verlag, Berlin/Heidelberg, v. 1465, p. 172–177, 1998. Disponível em: <http://www.springerlink.com/index/10.1007/BFb0055481>.

[71] FERGUSON, N.; SCHNEIER, B. *Practical cryptography*. [S.l.]: Wiley, 2003. ISBN 0471223573.

[72] MCDANIEL, P. D.; RUBIN, A. D. A response to "can we eliminate certificate revocation lists?". In: FRANKEL, Y. (Ed.). *Financial Cryptography*. [S.l.]: Springer, 2000. (Lecture Notes in Computer Science, v. 1962), p. 245–258. ISBN 3-540-42700-7.

[73] Jon B Alterman. *ISO/IEC 9798-3. Information technology - Security techniques - Entity authentication mechanisms - Part 3: Entity authentication using a public-key algorithm.* Geneva, Switzerland: [s.n.], 1993.

[74] ITI. *Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil*. v.3.0. Brasília, Dezembro 2008. DOC-ICP-04.

[75] SCHNEIER, B.; KELSEY, J. Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security (TISSEC)*, ACM, v. 2, n. 2, p. 159–176, 1999.

[76] HABER, S.; STORNETTA, W. S. How to time-stamp a digital document. In: *CRYPTO '90: Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 1991. p. 437–455. ISBN 3-540-54508-5.

[77] GONDROM, T.; BRANDNER, R.; PORDESCH, U. *Evidence Record Syntax (ERS)*. IETF, 2007. (Request for Comments). Disponível em: <http://www.ietf.org/rfc/rfc4998.txt>.

[78] SUN Microsystems. **Developer Resources for Java Technology**. Disponível em: <http://java.sun.com/>. Acesso em: 25/02/2010.

[79] **The Legion of the Bouncy Castle**. Disponível em: <http://www.bouncycastle.org/>. Acesso em: 25/02/2010.

[80] ITU-T. *Recommendation X.690 (11/2008) - Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*. 2008.

[81] THE PHP GROUP. **PHP: Hypertext Preprocessor**. Disponível em: <http://php.net/index.php>. Acesso em: 13/06/2010.

[82] FIELDING, R. et al. *Hypertext Transfer Protocol – HTTP/1.1*. IETF, jun. 1999. RFC 2616 (Draft Standard). (Request for Comments, 2616). Updated by RFC 2817. Disponível em: <http://www.ietf.org/rfc/rfc2616.txt>.

[83] The IEEE and The Open Group. *The Open Group Base Specifications Issue 6 – IEEE Std 1003.1, 2004 Edition*. New York, NY, USA: IEEE, 2004. Disponível em: <http://www.opengroup.org/onlinepubs/009695399/>.

[84] HOFFMAN, P. *Enhanced Security Services for S/MIME*. IETF, jun. 1999. RFC 2634 (Proposed Standard). (Request for Comments, 2634). Updated by RFC 5035. Disponível em: <http://www.ietf.org/rfc/rfc2634.txt>.

[85] PINKAS, D.; POPE, N.; ROSS, J. *Policy Requirements for Time-Stamping Authorities (TSAs)*. IETF, nov. 2003. RFC 3628 (Informational). (Request for Comments, 3628). Disponível em: <http://www.ietf.org/rfc/rfc3628.txt>.

[86] HARRINGTON, A.; JENSEN, C. Cryptographic access control in a distributed file system. In: ACM. *Proceedings of the eighth ACM symposium on Access control models and technologies*. [S.l.], 2003. p. 165.

[87] MICROSOFT. **The Microsoft .NET Framework**. Disponível em: <http://www.microsoft.com/net/>. Acesso em: 15/07/2010.

[88] THE OPENSSL PROJECT. **OpenSSL: The Open Source toolkit for SSL/TLS**. Disponível em: <http://www.openssl.org/>. Acesso em: 15/07/2010.

[89] ANSPER, A. et al. Efficient Long-Term Validation of Digital Signatures. In: *PKC '01: Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography*. London, UK: [s.n.], 2001. p. 402–415. ISBN 3-540-41658-7.