Infra-estrutura de Chaves Públicas Otimizada: Uma ICP de Suporte a Assinaturas Eficientes para Documentos Eletrônicos

Martín Augusto Gagliotti Vigil[1], **Nelson da Silva**[1], **Ricardo Moraes**[2], **Ricardo Felipe Custódio**[1]

[1] Laboratório de Segurança em Computação (LabSEC)
Universidade Federal de Santa Catarina
Caixa Postal 476 – 88040-900 – Florianópolis/SC – Brasil

[2]IT-Instituto de Telecomunicações, Universidade de Aveiro
Campus Universitário de Santiago – Aveiro – Portugal

Abstract. *In this work we have extended the ideas about Optimized Public Key Infrastructure (OPKI) and Optimized Certificates (OC) in such way: (1) an entity named Crypto Time is proposed to publish Novomodo proofs and then reducing operational costs of the OPKI's Root CA, (2) OC's validity interpretation is changed, (3) we expose a Relative Time Stamp implementation, (4) the users' trust in the Optimized Certificate Certification Authority is described, and (5) we present a new cost comparative that shows why the OC is an attractive alternative for long term archiving.*

Resumo. *Neste trabalho estendem-se as idéias sobre a Infra-estrutura de Chaves Públicas Otimizada (ICPO) e os Certificados Otimizados (CO) em vários aspectos: (1) propõe-se a entidade Crypto Time, responsável pela publicação das provas Novomodo, reduzindo assim o custo operacional da AC Raiz da ICPO, (2) apresenta-se uma modificação para a semântica da validade do CO, (3) aborda-se uma solução de Carimbo do Tempo Relativo, (4) descreve-se a confiança dos usuários na Autoridade Certificadora de Certificados Otimizados e (5) mostra-se, através de um novo comparativo de custos, por que o CO é uma atraente alternativa para arquivamento a longo prazo.*

1. Introdução

A Infra-estrutura de Chaves Públicas (ICP), inicialmente proposta por [Diffie and Hellman 1976], tem sido notavelmente empregada para prover a sistemas computacionais e a usuários funções de segurança como confidencialidade, integridade, autenticação e irretratabilidade. Entretanto, aplicações emergentes têm enfrentado desafios para implementar tais funções devido à complexidade da ICP. Por exemplo, redes sem fio industriais, redes de sensores e sistemas embarcados - todos com restrições de energia e processamento [Berbecaru et al. 2001, Dzung et al. 2005, Satizábal et al. 2007, Willig 2008].

Um aspecto relevante de complexidade da ICP é a validação de documentos assinados eletronicamente - processo que consiste em verificar a assinatura do documento e o caminho de certificação do signatário. Tal verificação é custosa por envolver procedimentos de busca e validação de certificados. Além disso, frequentemente informações

de status de revogação são necessárias e, para obtê-las, realizam-se consultas a servidores externos, estas sujeitas a problemas de disponibilidade e velocidade dos meios de comunicação. Adicionalmente, incluem-se carimbos do tempo com objetivo de fornecer referência temporal às assinaturas. Todavia, carimbos do tempo são também documentos assinados que exigem validação, aumentando ainda mais a complexidade do processo como um todo.

Como uma alternativa aos problemas citados, foi proposta a Infra-estrutura de Chaves Públicas Otimizada (ICPO) que emite Certificados Otimizados (CO) [Custódio et al. 2008]. Baseado na idéia de certificados de curta duração [Rivest 1998], o CO é válido para um instante específico i, ou seja, define-se no certificado X.509 os campos $notBefore = notAfter = i$. Portanto, um CO não é revogável. Adicionalmente, o CO funciona como um carimbo do tempo, uma vez que traz embarcado o resumo criptográfico de alguma informação (por exemplo, uma assinatura de documento). Por fim, o CO e seu caminho de certificação são utilizados para substituir o caminho de certificação original do signatário e os carimbos do tempo da assinatura, com o objetivo de reduzir a complexidade da validação de um documento assinado.

Este artigo amplia a proposta inicial sobre a ICPO [Custódio et al. 2008]. Desta forma, os fundamentos da ICPO são novamente abordados, porém, de maneira mais clara e, em seguida, as seguintes contribuições são apresentadas:

- inclusão da entidade Crypto Time para custódia das provas de validade Novomodo;
- modificação da semântica da validade do CO;
- implementação de Carimbo do Tempo Relativo incluindo provas Novomodo;
- descrição de uma alternativa eficiente para preservação de assinaturas por longo prazo;
- descrição do emprego da Autoridade Certificadora de Certificados Otimizados (ACCO) e sua relação de confiança com usuários;
- apresentação das equações de custos para comparação entre certificados convencionais e COs;
- descrição da inviabilidade de assinaturas auto-verificáveis com COs.

O restante deste trabalho está organizado na seguinte ordem: na Seção 2 apresentam-se a validação e a organização de documentos eletrônicos. A Seção 3 relata soluções na literatura que tratam os problemas de complexidade da ICP. A Seção 4 apresenta as características da ICPO, bem como sua vantagens. A Seção 5 aborda a ACCO na prática e suas relações de confiança com os usuários dentro de um domínio. A Seção 6 apresenta comparativos entre o uso de certificados convencionais e otimizados. Por fim, a Seção 7 expõe considerações sobre os COs propostos anteriormente e sobre as novas contribuições, finalizando este trabalho.

2. Conceitos Preliminares

A seguir descrevem-se a validação e os formatos de documento assinado, com o objetivo de fornecer base para o entendimento da otimização de documentos assinados proposta neste trabalho.

2.1. Validação de Assinatura

Para validar a assinatura de um documento é necessário verificar: a) a assinatura digital; b) o certificado 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 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 assinante 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. Para tal utiliza-se o algoritmo *Certificate Path Processing* [ITU-T 2005].

A construção do caminho de certificação consiste em encontrar pelo menos uma sequência de certificados de Autoridade Certificadora (AC) que ligue o certificado do signatário a um certificado confiável. Em seguida, para cada sequência encontrada verificam-se os certificados de acordo com:

- a integridade e a autenticidade da assinatura do certificado devem ser verificadas através da chave pública de seu emissor;
- o período de validade do certificado deve compreender o momento de criação da assinatura;
- o certificado 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 obedece a todas as políticas de certificação que sobre ele incidem dentro de sua respectiva ICP.

Os esquemas mais comuns de publicação de informações de revogação são *Lista de Certificados Revogados* (CRL) [Cooper et al. 2008] e *Online Certificate Status Protocol* (OCSP) [Myers et al. 1999]. No primeiro esquema, os verificadores obtém uma lista de status de revogação de certificados, a qual se encontra publicada em servidores. No segundo esquema, os verificadores devem contactar diretamente o emissor do certificado a ser verificado, ou ainda uma terceira entidade autorizada pelo emissor a fornecer informações de revogação. Todavia, tais consultas aumentam o tempo da validação do caminho de certificação devido a problemas de disponibilidade e velocidade de transferência de rede.

Vale citar que CRLs podem se tornar longas [Gutman 2002]. Por exemplo, após um ano de operação da ICP da Johnson & Johnson, sua CRL ultrapassou o tamanho de 1 megabyte [Guida et al. 2004]. Entretanto, este fato não ocorre no uso do OCSP, cujas informações de revogação são pequenas e específicas para um certificado. Adicionalmente, as informações fornecidas pelo servidor OCSP, bem como as CRLs, são documentos assinados e, portanto, são necessárias verificações para se garantirem integridade e autenticidade.

Em resumo, é evidente que a validação do caminho de certificação é um procedimento complexo cujo esforço computacional envolvido é intensificado pela presença de esquemas de revogação, além de ser proporcional ao comprimento do caminho de certificação [Martinez-Peláez et al. 2008]. Conclui-se, então, que o caminho de certificação ideal deveria ser livre de revogação de certificados e o mais curto possível

- por exemplo, uma ICP hierárquica em que a AC Raiz emite certificados para usuários finais. Entretanto, a possibilidade de revogação é uma realidade na maioria dos cenários e essa ICP apresenta a desvantagem de sobrecarregar a AC Raiz, além de expô-la a riscos de segurança.

2.2. Formatos de Documentos Assinados

O custo para armazenamento de documentos eletrônicos é dependente do conteúdo assinado como ainda da decisão de quais informações de validação embarcar. Para dar suporte ao armazenamento e promover interoperabilidade há padrões de documentos eletrônicos como *Cryptographic Message Syntax* (CMS) [Housley 2002], *CMS Advanced Electronic Signatures* (CAdES) [Signatures and (ESI) 2008a, Pinkas et al. 2008], entre outros.

Almejando baixo custo de armazenamento, pode-se optar pelo *CAdES-C*, no qual há apenas referências para as informações de validação, ficando a cargo do verificador obtê-las e, portanto, sujeito aos custos de transferência pela rede. Por outro lado, podem-se eliminar as consultas aos servidores que publicam status de revogação - por exemplo, para se obter uma CRL -, embarcando-se os dados de validação no documento assinado, como permite o *CAdES-X Long*. Contudo, provavelmente se pagará um alto preço pelo armazenamento.

Em cenários em que a validade de um documento assinado deve ser preservada por longos prazos, recomenda-se embarcar todos os dados de validação, caso contrário, obtê-los será um desafio para futuros verificadores. Prevendo tal recomendação, há o padrão *CAdES-A*, que ainda permite a adição contínua de novos carimbos do tempo ao longo dos anos, os quais também exigem dados de validação embarcados. Portanto, a preservação a longo prazo demanda uma quantidade sempre crescente de recursos, pois a quantidade de dados de validação embarcados no documento assinado aumenta com passar do tempo.

Por fim, destaca-se a relação inversa entre custos de armazenamento e de transferência pela rede dos dados de validação. Em nosso ponto de vista, o ideal seria um documento assinado auto-verificável cujas informações de validação fossem reduzidas e embarcadas. Entretanto, tal cenário ainda é um problema em aberto. Já o armazenamento a longo prazo ideal deveria apresentar custo constante ao passar do tempo, o que pode ser obtido conforme apresenta este trabalho.

3. Trabalhos Relacionados

As fontes de complexidade mencionadas na Seção 2 são tema de discussão há anos, em especial os problemas de revogação e das CRLs. Focando a baixa escalabilidade e alto custo das CRLs há diversas propostas relevantes na literatura: *Delta CRL* [ITU-T 2005], *CRL Distributed Points* [ITU-T 2005], *Windowed CRL* [Mcdaniel et al. 2000], *Over-issued CRL* [Cooper 1999], *Blacklist CRL* [Perlman and Kaufman 1993], *Redirected Pointers* [Adams and Zuccherato 1998], *Certificate Revocation Trees* [Kocher 1998] e *Certificate Revocation Status* (CRS), também conhecido como Novomodo [Micali 2002].

O método Novomodo é extremamente eficaz na determinação do status de revogação de um certificado. As informações de status de revogação são formadas por valores de resumo criptográfico, portanto, são de tamanho fixo e reduzido. Além disso, sua autenticidade dispensa o uso de assinatura por parte do emissor, pois para sua falsificação é necessária a inversão da função de resumo criptográfico, algo computacionalmente

inviável. Devido a essas características, o método Novomodo representa uma atraente solução de revogação para sistemas com restrições de recursos computacionais tais como redes *ad-hoc* móveis.

Por outro lado, há a proposta de se desprezar a possibilidade de revogação e, por consequência, suas desvantagens desapareceriam. Baseados nesta idéia estão os certificados de curta duração [Rivest 1998] cujo tempo de vida é tão reduzido – por exemplo, 1 dia – que a probabilidade de serem revogados é praticamente desprezível. Estes esquemas são empregados na *Infra-estrutura Simples de Chaves Públicas* (SPKI) [Ellison 1999, Ellison et al. 1999]. Entretanto, tais certificados são úteis para usuários finais, não sendo práticos para ACs.

Outros trabalhos buscaram otimizar o número de operações criptográficas para se verificar o caminho de certificação. Em destaque estão os certificados aninhados [Levi et al. 2004]. Este esquema de certificação 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.

Adicionalmente, há a possibilidade de se delegar a tarefa de validação do caminho de certificação para entidades denominadas verificadores. Exemplos de verificadores são OCSP, OCSP-X [Hallam-Baker 1999], *Simple Certificate Validation Protocol* (SCVP) [Freeman et al. 2007], e *Data Validation and Certification Server Protocol* (DVCS) [Adams et al. 2001].

4. Infra-estrutura de Chaves Públicas Otimizada

A Figura 1 ilustra a Infra-estrutura de Chaves Públicas Otimizada: uma ICP convencional contendo uma Autoridade Certificadora de Certificados Otimizados responsável por emitir Certificados Otimizados. Os objetivos da ICPO são: a) minimizar os dados de validação em documentos assinados; b) reduzir o custo da validação da assinatura do documento.

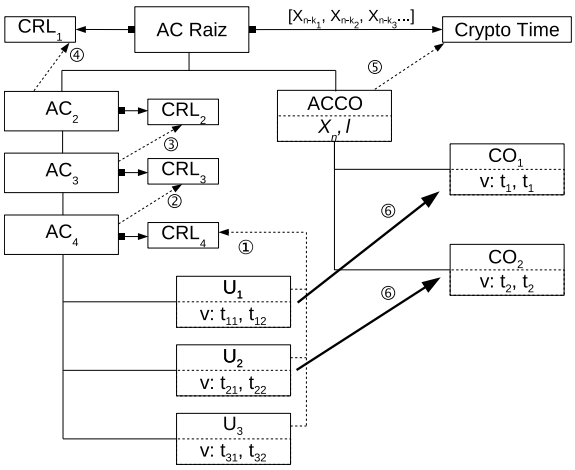

Figura 1. ICP Otimizada.

O CO é um certificado de curta duração, entretanto com uma sutil diferença ao modelo proposto em [Rivest 1998]: a validade de um CO corresponde ao instante i em

que ele foi emitido, ou seja, os campos *notBefore* e *notAfter* do certificado X.509 são iguais a i. Devido a esta característica, não há razão para se revogar um CO, pois se ele foi emitido, ele era válido no momento da emissão.

Emite-se um CO para a assinatura de um documento com o objetivo de se substituírem as informações originais necessárias para validá-la (caminho de certificação, status de revogação e carimbos do tempo). Devido ao caminho de certificação do CO ser otimizado, a verificação da assinatura do documento se dá de forma mais rápida. Entretanto, é necessária a prévia validação da assinatura do documento para que não se emita um CO válido para uma assinatura inválida. Uma vez garantida essa validade, emite-se um CO cujos titular e chave pública são copiados do certificado do signatário.

Uma vez que o CO vale somente para um instante particular de tempo, pode-se utilizá-lo também como carimbo do tempo da assinatura de um documento. Para tal, basta embarcar o resumo criptográfico da assinatura. Outra vantagem é que um CO pode ser facilmente substituído por outro em contra-partida ao envelhecimento dos algoritmos criptográficos. Portanto, é possível estender o tempo de vida da assinatura de documentos eletrônicos sem aumentar os dados de validação como mencionado na Seção 2.2.

Para dar suporte à emissão de COs há a Autoridade Certificadora de Certificados Otimizados e o Crypto Time, ambos ilustrados na Figura 1. Nesta, observa-se também a existência de certificados tradicionais (U_1, U_2, U_3) e otimizados (CO_1, CO_2) na ICPO. Os números de 1 a 5 referem-se ao relacionamento entre certificados e a fonte de consulta de status de revogação. Número 5 mostra a ACCO solicitando seu status de revogação ao Crypto Time, que é responsável pela custódia da provas de validade Novomodo (X_{n-k}) [Micali 2002] produzidas pela AC Raiz. Número 6 destaca a relação entre certificados tradicionais e otimizados, cujas validades referem-se, respectivamente, a um período de tempo e a um instante particular. Por fim, há dois valores embarcados no certificado da ACCO, relativos aos seguintes parâmetros do esquema Novomodo [Micali 2002]: alvo de validação (X_n) e granularidade (l).

A ACCO opera como um serviço notarial online para o qual usuários submetem dados de documentos assinados cujas informações de validação desejam otimizar. Assim os usuários fornecem à ACCO resumos criptográficos, assinaturas e respectivos carimbos do tempo, caminhos de certificação dos signatários e dados de revogação. Por sua vez, a ACCO valida, de acordo com os dados submetidos, os documentos assinados e retorna COs. Ademais, a fim de que o caminho de certificação do CO seja o mais curto possível, o certificado da ACCO é emitido pela AC Raiz.

Portanto, neste caso, há um baixo custo de validação do CO. Consequentemente, se for considerado o certificado da AC Raiz como uma âncora de confiança, então despreza-se a checagem de revogação para tal certificado. Tal premissa reduz ainda mais o custo de validação do caminho de certificação do CO, pois apenas o status de revogação da ACCO é verificado, e de maneira eficiente através de Novomodo. Por fim, garante-se a aderência do CO ao padrão X.509, não havendo mudanças estruturais do formato, sendo que as informações adicionais - por exemplo, Novomodo, resumo criptográfico para função de carimbo do tempo - são embarcadas através de extensões previstas no X.509v3.

4.1. Esquemas de Revogação na ICPO

Devido à ICPO ser uma ICP convencional com alguns ramos otimizados, diferentes formas de revogação podem ser adotadas. Para os caminhos de certificação tradicionais aplicam-se soluções baseadas em CRL e OCSP. Por outro lado, os caminhos de certificação otimizados, compostos pelo certificado da ACCO e por um CO, utilizam o esquema de revogação Novomodo.

Em [Custódio et al. 2008] foi proposto que a AC Raiz seria responsável por criar e manter sob sigilo os valores secretos X_0 e Y_0, como ainda gerar e publicar, através do CRS, as provas Novomodo (X_{n-k} e Y_1). Nesse contexto, faz-se interessante, a primeira vista, que a emissão do CRS aconteça no mesmo momento e na mesma frequência que a emissão de CRL_1 (Figura 1), não impactando nos custos operacionais já elevados de uma AC Raiz, que normalmente opera de maneira offline. Todavia, devido à ACCO ser um serviço online cuja chave privada é constantemente utilizada, sua exposição a ameaças de segurança é maior e, portanto, a emissão de status de revogação para seu certificado deve ocorrer a uma frequência mais elevada. Tal fato obriga a AC Raiz a ser utilizada também a uma frequência maior e, consequentemente, incrementa seu custo operacional. Como solução a este problema, propõe-se o uso do Crypto Time.

Neste caso, a AC Raiz produz previamente todas as provas de validade Novomodo (X_{n-k}) que serão publicadas durante o período de validade da ACCO, cujo certificado está prestes a ser emitido. Em seguida, logo após a AC Raiz emitir o certificado da ACCO, as provas de validade são transferidas de maneira segura ao Crypto Time, que deverá mantê-las sob sigilo. Tais provas são, então, liberadas pelo Crypto Time gradativamente, ao longo da vida da ACCO, mediante prévia autorização de auditores da ICPO, que atestam a integridade da ACCO naquele período.

Verificadores averiguam o status de revogação da ACCO por meio do método Novomodo, cujos valores de entrada são apenas o alvo de validade (X_n) e a prova de validade (X_{n-k}), obtidos no certificado da ACCO e no repositório público do Crypto Time, respectivamente. Porém, o leitor pode questionar que a prova de revogação (Y_1) deve ser também verificada segundo o algoritmo de Novomodo. Contudo, justifica-se a ausência da prova de revogação devido aos papéis do Crypto Time e dos auditores: a retenção da próxima prova de validade ($X_{n-(k+1)}$) por parte do Crypto Time bloqueia as operações da ACCO imediatamente após a expiração da prova de validade atual (X_{n-k}). Além disso, descarta-se a possibilidade de se forjar $X_{n-(k+1)}$, fato sustentado pela inviabilidade computacional da inversão de funções de resumo criptográfico.

4.2. Referência Temporal para Validação de Assinatura

De acordo com [Custódio et al. 2008], o CO é um certificado válido para um instante particular i que pode corresponder, por exemplo, ao momento em que a assinatura de um documento foi criada ou foi aceita como válida por uma terceira parte. Contudo, não se fizeram restrições a i, sendo possível, por exemplo, que a validade do CO corresponda a um momento que antecede o início da validade de seu emissor, a ACCO. Tal cenário é indesejável, uma vez que contradiz a semântica da validade de certificados X.509.

Sugere-se então que i corresponda ao momento em que a ACCO emitiu o CO, porém deve-se embarcar no CO a referência temporal utilizada pela ACCO para validar a

assinatura do documento submetido. As possibilidades para tal referência são apresentadas na Tabela 1. No primeiro caso ($N = 1$) a validação é efetuada no momento em que o CO foi solicitado por um usuário. Em $N = 2$ a validação ocorre no instante informado por um carimbo do tempo da assinatura do documento. Em $N = 3$ a referência de tempo para validação é obtida de um CO prévio. Em $N = 4$ a referência de tempo equivale ao momento em que a assinatura foi criada e, neste caso, o solicitante do CO deve ser o signatário do documento. Por fim, em $N = 5$ a referência é informada pelo usuário solicitante de CO, não necessariamente o signatário, correspondendo ao momento em que ele concorda com a assinatura do documento.

Tabela 1. Referência de tempo para validação de assinatura.

N	Referência	Fonte de Tempo
1	Instante de requisição do CO	Relógio interno da ACCO
2	Passado	Um carimbo de tempo da assinatura
3	Passado	Um CO prévio
4	Passado	Signatário do documento
5	Passado	Um verificador do documento

4.3. Carimbo do Tempo Relativo

Em [Custódio et al. 2008] foi proposta a utilização de Carimbo do Tempo Relativo [Haber and Stornetta 1991] de forma a dar suporte ao trabalho de auditoria sobre a ACCO. Apresenta-se a seguir um aprimoramento de tal proposta, sugerindo-se a inserção das provas de validade Novomodo (X_{n-k}) na sequência de resumos criptográficos do Carimbo do Tempo Relativo com o objetivo de ordenar os COs sobre os períodos do método Novomodo [Micali 2002].

Ao longo de seu tempo de vida, a ACCO mantém uma sequência única que contém o resumo criptográfico de cada CO emitido. Tal sequência é segmentada em $\frac{n}{l}$ períodos, sendo n o tempo de validade da ACCO (por exemplo, 365 dias) e l a granularidade - tempo para emissão de status de revogação (por exemplo, 30 dias). 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 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 período $k - 1$ antes de serem inseridas na sequência, de modo a delimitar o final deste 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 2 ilustra o 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.

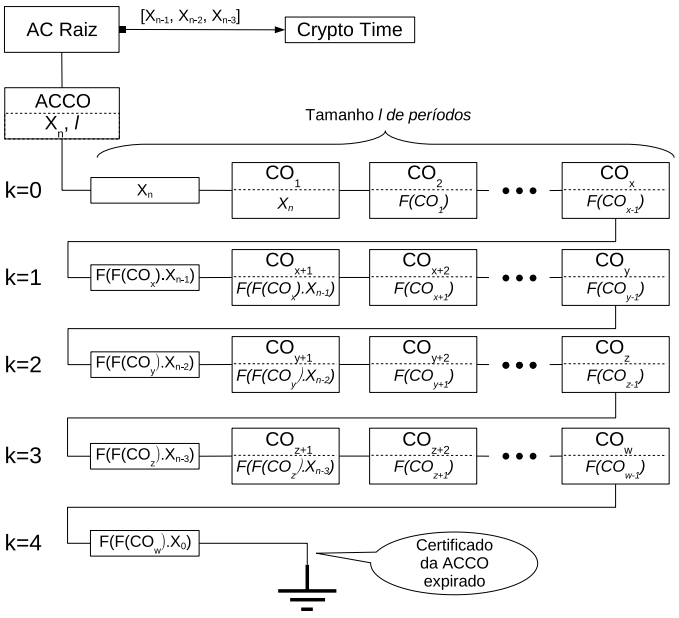

Figura 2. Carimbo do Tempo Relativo incluindo provas Novomodo.

O uso das provas X_{n-k} proporciona informação adicional ao Carimbo do Tempo Relativo, possibilitando que se saiba em qual dos $\frac{n}{l}$ períodos um CO foi emitido. Além disso, essas provas podem ser vistas como referências de tempo no qual se garante que, até o momento da publicação de X_{n-k}, a ACCO estava íntegra, o que permitiria a identificação de COs legítimos emitidos antes de um possível comprometimento da ACCO. Adicionalmente, sugere-se que o Carimbo do Tempo Relativo seja mantido em um ambiente seguro e armazenado em uma mídia especial com a propriedade de que dados escritos não podem ser modificados posteriormente, caso contrário um adversário poderia reproduzir uma sequência falsa utilizando as provas publicadas antes do ataque.

4.4. 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 [Signatures and (ESI) 2008b] e *Evidence Record Syntax* (ERS) [Gondrom et al. 2007]. 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 de arquivamento como os COs estão sujeitos aos problemas de enfraquecimento dos algoritmos criptográficos, bem como a expiração dos prazos de validade relativos aos caminhos de certificação. Entretanto, ao contrário de um carimbo do tempo de arquivamento, 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.

5. Emprego da ACCO

Considera-se a ACCO um serviço notarial online cujos COs emitidos são restritos a documentos assinados dentro da mesma ICP hierárquica em que a ACCO se encontra. Além disso, é importante citar que CO é uma evidência de que o certificado do signatário foi validado pela ACCO. Entretanto cabe aos usuários confiar ou não nessa validação. De forma a ilustrar tal relação de confiança descreve-se o uso da ACCO dentro de domínios bem delimitados.

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

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

Em 5 ilustra-se a ocasião em que se rejeita a entrada de um documento assinado otimizado cujo CO em anexo foi emitido por uma ACCO desconhecida. Isso ocorre pois nesse domínio decidiu-se por não se confiar em ACCOs externas, como ainda não há os dados originais de validação para verificar a veracidade do CO.

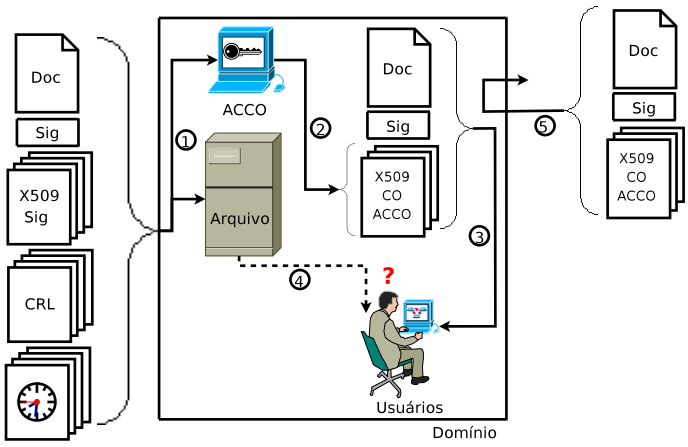

Figura 3. Emprego da ACCO em um domínio.

Uma vez que usuários externos ao domínio podem desconhecer a ACCO, sugere-se desfazer a otimização de um documento assinado antes de enviá-lo para fora do

domínio. Dessa maneira, caberia ao usuário solicitar ao Arquivo os dados originais de validação e, em seguida, anexá-los ao documento assinado, removendo o caminho de certificação otimizado.

Por fim, tal esquema permite a um domínio economizar quantidades significativas de recursos, em especial se há um conjunto de documentos assinados que circula pela rede interna e é utilizado diversas vezes por vários usuários.

6. Custos Computacionais

Os custos computacionais abordados referem-se ao total de recursos e de esforço necessários para armazenar e verificar, respectivamente, um documento assinado. Os custos são apresentados na forma comparativa na Tabela 3, cujas variáveis são definidas na Tabela 2.

Tabela 2. Parâmetros para cálculos de custo.

Parâmetro	Descrição
N_{sig}	Número de certificados no caminho de certificação do signatário
N_{ACT}	Número de certificados no caminho de certificação de uma ACT
P	Período em que uma assinatura é mantida válida
V	Período médio de validade de certificado de ACTs
R	Informação de revogação
C	Certificado X.509
S	Função de resumo criptográfico para geração de provas Novomodo
n	Tempo de validade da ACCO
l	Granularidade do método Novomodo
m	Número de vezes em que se utiliza um documento assinado

Tabela 3. Custos envolvidos no uso de certificados tradicionais e otimizados.

Custo	Certificado Tradicional	Certificado Otimizado
Verificação	$m(2 \times N_{sig} + 2 \times \frac{P}{V} \times N_{ACT} + \frac{P}{V} + 1)$	$m[3 + (\frac{n}{l} - 1) \times S]$
Armazenamento	$N_{sig} \times C + N_{sig} \times R + \frac{P}{V} \times N_{ACT} \times C + (\frac{P}{V} - 1) \times N_{ACT} \times R + \frac{P}{V}$	$2 \times C$

O custo de verificação leva em consideração a quantidade de vezes que um documento assinado é utilizado (m) e quantas assinaturas precisam ser verificadas para garantir a autenticidade, a integridade e a irretratabilidade da assinatura do documento. Desta maneira, devem-se considerar as assinaturas dos seguintes conteúdos: a) certificados e informações de revogação do caminho de certificação do signatário ($2 \times N_{sig}$); b) certificados e informações de revogação do caminho de certificação da Autoridade de Carimbo do Tempo (ACT) ($2 \times N_{ACT}$); c) carimbos do tempo ($\frac{P}{V}$); d) o documento (1) . Por outro lado, o custo de verificação de um documento assinado com CO em anexo é constante e proporcional a validar 3 assinaturas - referentes ao documento assinado, ao CO e ao certificado da ACCO - e executar um algorítmo de resumo criptográfico S, no pior caso do método Novomodo, $\frac{n}{l} - 1$ vezes.

Já o custo de armazenamento consiste em contabilizar os certificados (C) e respectivas informações de revogação (R) relativos aos caminho de certificação do signatário

e das ACTs, como ainda os carimbos do tempo ($\frac{P}{V}$). As informações de revogação relativas ao emissor do último carimbo do tempo adicionado ao documento assinado não são contabilizadas nos custos de armazenamento, pois elas precisam ser atuais no momento da verificação da assinatura. Portanto, tais informações são obtidas através de consultas às fontes que publicam o status de revogação do emissor do carimbo do tempo. Por outro lado, o custo envolvido no armazenamento de um documento assinado com CO em anexo é constante e proporcional a 2 certificados: o otimizado e o da ACCO.

Por fim, fica claro a redução dos custos computacionais quando o CO é empregado. Contudo, nota-se que a minimização do esforço favorece aos verificadores, e não ao signatário. Todavia, é importante lembrar que o signatário verifica uma única vez a validade de seu certificado antes de assinar um documento, enquanto verificadores podem utilizar o mesmo documento assinado diversas vezes e, em todas, devem validar a assinatura e o certificado do signatário.

7. Considerações

Visando a aderência ao padrão de certificados X.509, buscou-se em [ITU-T 2005] e [Cooper et al. 2008] a existência de alguma restrição que impedisse a equivalência entre o valor dos campos *notBefore* e *notAfter* - uma das características principais do CO. Em ambas as referências não existe um período de validade mínimo para os certificados. Em seguida, implementaram-se em Java uma versão simplificada da ACCO e uma aplicação cliente para solicitar COs para documentos assinados em formato CMS. Tal aplicação foi ainda capaz de validar um documento assinado otimizado fazendo uso da implementação do *Certificate Path Processing* presente na Máquina Virtual Java.

A substituição do certificado original do signatário por um CO, cuja chave pública é a mesma do primeiro, possui as mesmas características de um ataque de substituição. Para prevenir este ataque, em alguns formatos de documento eletrônico (por exemplo, CAdES) o signatário pode incluir o resumo criptográfico de seu certificado como atributo autenticado, impedindo a substituição de certificado. Por consequência, tal funcionalidade impede o uso de COs.

Em [Custódio et al. 2008] há uma lacuna a respeito do uso das provas de validade Novomodo. Embora seja impossível para um adversário forjar uma prova, ele é capaz de, após comprometer a ACCO, utilizar provas X_{n-k} expiradas e emitir COs forjados cujas validades remetem ao passado sem que partes confiantes percebam a fraude. Mesmo que seja usado o Carimbo do Tempo Relativo proposto em 4.3, um verificador pode não perceber a fraude, uma vez que ele considera o documento assinado como auto-verificável e, assim, dispensa consultas externas. Portanto, o conceito de documento assinado auto-verificável através de Novomodo é apenas válido se considerarmos a premissa de que é impossível o comprometimento da chave privada da ACCO. Embora esse cenário seja pouco provável, há ainda a revogação de certificado por outros motivos e a cessão de provas de Novomodo seria útil para inibir automaticamente a operação de uma ACCO sem que os administradores precisassem efetivamente desligá-la.

Por fim, fica a sugestão de que se realizem estudos comparativos de desempenho na verificação de caminhos de certificação tradicionais e otimizados, além de explorar as limitações apresentadas aqui, de forma a conceber informações auto-verificáveis de validação assinatura.

Referências

Adams, C., Sylvester, P., Zolotarev, M., and Zuccherato, R. (2001). Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols. RFC 3029 (Experimental).

Adams, C. and Zuccherato, R. (1998). A general, flexible approach to certificate revocation. Entrust Technologies White Paper.

Berbecaru, D., Lioy, A., and Marian, M. (2001). On the complexity of public-key certificate validation. In *ISC '01: Proceedings of the 4th International Conference on Information Security*, pages 183–203, London, UK. Springer-Verlag.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W. (2008). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (Proposed Standard).

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

Custódio, R. F., Vigil, M. A., Romani, J., Pereira, F. C., and Silva Fraga, J. (2008). Optimized certificates — a new proposal for efficient electronic document signature validation. In *EuroPKI '08: Proceedings of the 5th European PKI workshop on Public Key Infrastructure*, pages 49–59, Berlin, Heidelberg. Springer-Verlag.

Diffie, W. and Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654.

Dzung, D., Naedele, M., Von Hoff, T., and Crevatin, M. (2005). Security for industrial communication systems. *Proceedings of the IEEE*, 93(6):1152–1177.

Ellison, C. (1999). SPKI Requirements. RFC 2692 (Experimental).

Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., and Ylonen, T. (1999). SPKI Certificate Theory. RFC 2693 (Experimental).

Freeman, T., Housley, R., Malpani, A., Cooper, D., and Polk, W. (2007). Server-Based Certificate Validation Protocol (SCVP). RFC 5055 (Proposed Standard).

Gondrom, T., Brandner, R., and Pordesch, U. (2007). Evidence Record Syntax (ERS). RFC 4998 (Proposed Standard).

Guida, R., Stahl, R., Bunt, T., Secrest, G., and Moorcones, J. (2004). Deploying and using public key technology: Lessons learned in real life. *IEEE Security and Privacy*, 2(4):67–71.

Gutman, P. (2002). Pki: It's not dead, just resting. *Computer*, 35(8):41–49.

Haber, S. and Stornetta, W. S. (1991). How to time-stamp a digital document. In *CRYPTO '90: Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*, pages 437–455, London, UK. Springer-Verlag.

Hallam-Baker, P. (1999). OCSP Extensions. Work in progress, IETF PKIX working group.

Housley, R. (2002). Cryptographic Message Syntax (CMS). RFC 3369 (Proposed Standard). Obsoleted by RFC 3852.

ITU-T (2005). Recommendation X.509 information technology - open systems interconnection - the directory: Authentication framework. Technical report, ITU-T.

Kocher, P. C. (1998). On certificate revocation and validation. *Financial Cryptography*, 1465:172–177.

Levi, A., Caglayan, M. U., and Koc, C. K. (2004). Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure. *ACM Trans. Inf. Syst. Secur.*, 7(1):21–59.

Martinez-Peláez, R., Satizábal, C., Rico-Novella, F., and Forné, J. (2008). 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*, pages 701–708, Washington, DC, USA. IEEE Computer Society.

Mcdaniel, P., Jamin, S., and Arbor, A. (2000). Windowed key revocation in public key infrastructures. *IEEE INFOCOM*, 3:1406–1414.

Micali, S. (2002). NOVOMODO: Scalable Certificate Validation and Simplified PKI Management. In *Proceedings of the 1st Annual PKI Research Workshop*, NIST, Gaithersburg MD, USA.

Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C. (1999). X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560 (Proposed Standard).

Perlman, R. and Kaufman, C. (1993). Method of issuance and revocation of certificates of authenticity used in public key networks and other systems. Technical report, United State Patent 5,261,002.

Pinkas, D., Pope, N., and Ross, J. (2008). CMS Advanced Electronic Signatures (CAdES). RFC 5126 (Informational).

Rivest, R. L. (1998). Can we eliminate certificate revocations lists? In *FC '98: Proceedings of the Second International Conference on Financial Cryptography*, pages 178–183, London, UK. Springer-Verlag.

Satizábal, C., Hernández-Serrano, J., Forné, J., and Pegueroles, J. (2007). Building a virtual hierarchy to simplify certification path discovery in mobile ad-hoc networks. *Comput. Commun.*, 30(7):1498–1512.

Signatures, E. T. C. E. and (ESI), I. (2008a). Electronic signatures and infrastructures (esi); cms advanced electronic signatures (cades). Technical report, European Telecommunications Standards Institute.

Signatures, E. T. C. E. and (ESI), I. (2008b). Electronic signatures and infrastructures (esi); profiles of xml advanced electronic signatures based on ts 101 903 (xades). Technical report, European Telecommunications Standards Institute.

Willig, A. (2008). Recent and emerging topics in wireless industrial communications: A selection. *IEEE Transactions on Industrial Informatics*, 4(2):102–124.