Certificados Otimizados para a validação eficiente da Assinatura Digital

Adriana Elissa Notoya[1], **Ricardo Felipe Custódio**[2]
Fernando Carlos Pereira[1], **Joni da Silva Fraga**[1]

[1]Programa de Pós-Graduação em Engenharia Elétrica (PPGEEL)
Universidade Federal de Santa Catarina (UFSC)
Caixa Postal 476 – 88040-900 – Florianópolis – SC – Brasil

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

custodio@inf.ufsc.br, {elissa,fernando,fraga}@das.ufsc.br

Abstract. *This paper proposes optimized digital certificates as a way to efficiently sign and verify the signatures of electronic documents. Both verification efficiency and the elimination of revocation are advantages of optimized certificates, making them suitable for hierarchical PKIs of wireless applications.*

Resumo. *Este trabalho propõe certificados otimizados para a verificação eficiente de assinatura digital de documentos eletrônicos. Os certificados omitizados podem ser utilizados em substituição ao certificado do signatário como meio de comprovar a validade de assinaturas digitais. A melhoria na verificação da assinatura, a eliminação da necessidade de se verificar o status do certificado e de um carimbo de tempo de uma terceira parte são vantagens do certificado otimizado, tornando-os adequados a aplicações, por exemplo, em dispositivos wireless.*

1. Introdução

Este trabalho propõe um método eficiente para validação da assinatura de documentos eletrônicos através do uso de um novo tipo de certificado digital. Trata-se do *certificado otimizado*, que é utilizado em substituição ao certificado digital do signatário[Zhou and Deng 2000], sem modificar o esquema tradicional de emissão de certificados digitais dos assinantes. Adicionalmente, o certificado otimizado tem a vantagem de poder ser utilizado como carimbo do tempo da assinatura ou do instante de tempo onde a assinatura foi verificada como válida. O método proposto é ideal para sistemas computacionais sob condições especiais de energia limitada (aplicações em wireless, redes ad-hoc, etc.).

A Seção 2 apresenta em detalhes o conceito de certificados otimizados, seus benefícios e principais aplicações. A Seção 3 introduz a autoridade certificadora otimizadora e os procedimentos adotados para emissão dos certificados otimizados. A Seção 4 contém a conclusão do artigo e algumas sugestões de trabalhos futuros.

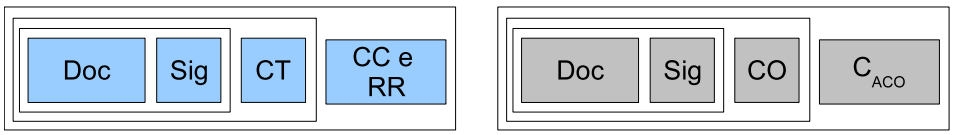
2. Certificados Otimizados

O Certificado Otimizado (CO) pode ser visto como *um certificado emitido para um documento assinado*. Este certificado substitui o conjunto de informações necessário para validação de uma assinatura, visando tornar esse procedimento mais eficiente, através da minimização do processamento redundante tradicionalmente necessário nessa operação.

Os COs são emitidos, por uma entidade denominada Autoridade Certificadora Otimizadora (ACO), uma única vez para cada documento e no processo de validação da assinatura substitui o certificado tradicional. O certificado convencional é utilizado apenas no processo de requisição do certificado otimizado.

Os elementos do esquema tradicional de assinatura são mostrados na Figura 1 a). Nesta figura *Doc* é o documento eletrônico, *Sig* é a assinatura digital e *CT* é o carimbo do tempo. *CC* corresponde à cadeia de certificação, formada pelos certificados do signatário e de todos os certificados do caminho de certificação entre a AC emissora do certificado do signatário e o certificado da AC Raiz[Housley and Polk 2001]. *RR* constitui as listas de certificados revogados de *CC*. A Figura 1 b) apresenta o esquema de assinatura com certificado otimizado: *Doc*, *Sig*, certificado otimizado (*CO*) e o certificado C_{ACO} da ACO.

Comparando-se as duas representações da Figura 1 pode-se constatar que o *CT*, *CC* e o *RR* do método tradicional de assinatura são substituídos por somente dois certificados: o C_{ACO} e o CO.



(a) Tradicional. (b) Assinatura com CO.

Figura 1. Assinatura digital de documentos eletrônicos.

A Figura 2 ilustra um cenário possível para a implantação de uma ACO. A ACO localizada no topo de uma ICP hierárquica com 4 níveis cujos usuários possuem documentos assinados através do certificado convencional. As assinaturas desses documentos podem ser validados tanto pelo caminho tradicional, com 4 certificados ou pelo CO com apenas 2.

Para a emissão de um CO, a ACO deve verificar a assinatura e validar todo o caminho de certificação do certificado do usuário como no método convencional. Estando as informações válidas, o CO é emitido, cujas informações básicas são:

- *informações do certificado convencional utilizado para realizar a assinatura*: para identificação do signatário do documento;
- *período de validade igual a* k: tempo de início e fim da validade iguais ao instante da conferência realizada pela ACO para emitir o CO;
- *hash do documento*: relaciona de forma única o CO a um documento;
- *flag* f: indica se o requisitante da emissão do CO é o signatário ou um conferente.

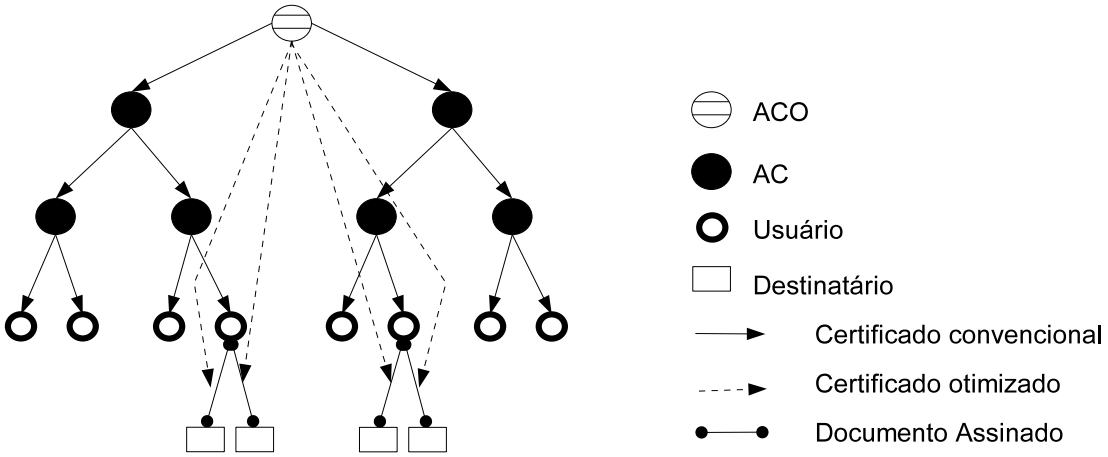


Figura 2. ICP com ACO.

O CO é uma evidência de que a assinatura era válida no tempo k. Assim, todos os usuários que necessitem verificar essa assinatura conferem apenas a validade desse certificado. Isso elimina a redundância do processo.

O parâmetro f, que indica qual é o usuário solicitante, signatário ou validador, estabelece o modo como o período de validade do certificado deve ser interpretado. O objetivo de um validador em substituir o certificado original do signatário por um CO é otimizar posteriores validações da assinatura de um documento.

3. Autoridade Certificadora Otimizadora

A Autoridade Certificadora Otimizadora tem as funções de conferir a assinatura, validar o certificado do signatário e emitir o CO.

A localização da ACO no topo da hierarquia da ICP (Fig. 3.a), é devido a necessidade de reduzir o caminho de certificação. Entretanto, minimizar a exposição da chave privada da AC Raiz, propõe-se estabelecer a ACO como uma AC subordinada, no nível 2 da hierarquia, (Fig. 3.b).

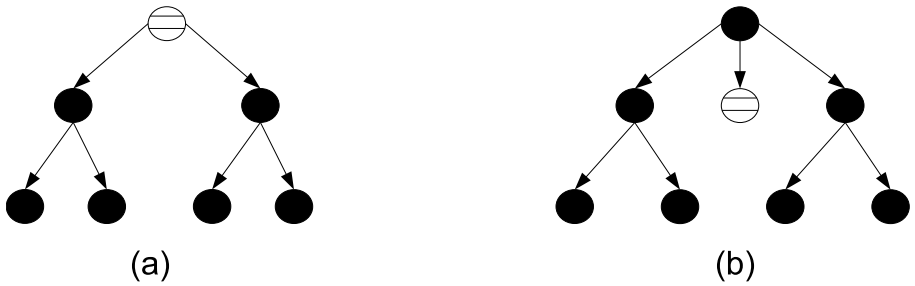


Figura 3. ICP com ACO.

A validade do certificado da ACO pode ser eficientemente tratada por uma adaptação do método proposto por Silvio Micali [Micali 1996]. Este método elimina a necessidade de se utilizar uma Lista de Certificados Revogados (LCR)[Jain 2005].

Micali trabalha com dois valores escolhidos de forma aleatória, Y_0 e N_0 e uma

função de hash F como meio para provar que um certificado era válido num determinado instante de tempo t. A resolução de validade l é o intervalo de tempo entre uma possível revogação e outra. Em t haverá $n = t * l$ intervalos de tempo. n equivale a quantidade de vezes que a informação do status do certificado será publicada. Essas informações são publicadas em um *Lista de Status dos certificados* (LSC).

Os parâmetros do método devem ser definidos pela AC Raiz. Em seguida, N_1 é calculado: $N_1 = F(N_0)$. Uma cadeia é calculada com o valor de Y_0, através da submissão a função H n vezes: $Y_1 = F(Y_0), Y_2 = F(Y_1), ..., Y_n = F(Y_{n-1})$. A AC Raiz, mantém secretos os valores de Y_0 e N_0 e inclui os valores de Y_n e N_1 no certificado da ACO. O valor de Y_n é utilizado para conferir se o certificado encontra-se válido.

A AC Raiz insere Y_{n-k} na LSC se o certificado não encontra-se revogado. Caso contrário, para revogar, a AC Raiz deve inserir N_0 nesta lista. A LSC é então assinada, datada e publicada pela AC Raiz.

Para verificar se o certificado da ACO é válido em um determinado intervalo de tempo k, deve-se obter da LSC o valor de Y_{n-k}. Se $F(Y_{n-1}) = Y_n$, onde Y_n é obtido do certificado da ACO, então tem-se a garantia de que o certificado era válido em k.

Caso um determinado período de tempo k não possua o valor correspondente Y_{n-k} na LSC, a ACO não pode provar que seu certificado é válido neste período. A ACO deve então verificar se N_0 consta na LSC. A revogação pode ser verificada determinando-se $N = F(N_0)$, onde N_0 deve estar na LSC e N no certificado da ACO.

A ACO, ao emitir um CO, consulta a LSC na AC Raiz e obtém a prova de que a mesma é válida e a insere no CO. Assim, o CO além de ser inerentemente válido, pois era válido quanto foi emitido, possui em seu corpo uma prova de que o certificado da ACO era também válido no mesmo momento em que o CO foi emitido. A prova de que o certificado da ACO é válido é o parâmetro Y_{n-k} do método de Micali que permite verificar o status de um certificado no instante k.

4. Conclusão

Os certificados otimizados possibilitam um ganho considerável de eficiência no processo de verificação da assinatura dos documentos eletrônicos. A sobrecarga dessa operação é reduzida devido a minimização da redundância do processo e da cadeia de certificação associado ao certificado do signatário.

As característica de auto validação e baixa sobrecarga de processamento torna o CO uma forma eficiente de distribuir documentos eletrônicos assinados em redes ad hoc, cujo os nós possuem recursos limitados, principalmente de memória e processamento.

Referências

Housley, R. and Polk, T. (2001). *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*. John Wiley & Sons, Inc., New York, NY, USA.

Jain, G. (2005). Certificate revocation: a survey. http://www.cis.upenn.edu/ jainq/papers/recocation.pdf.

Micali, S. (1996). Efficient certificate revocation. Technical report, Cambridge, MA, USA.

Zhou, J. and Deng, R. (2000). On the validity of digital signatures. *SIGCOMM Comput. Commun. Rev.*, 30(2):29–34.