Melhores práticas para substituição de Autoridades Certificadoras em uma ICP

Marcelo Carlomagno Carlos, Ricardo Felipe Custódio

8 de Outubro de 2006

Resumo

A melhor forma de gerência do ciclo de vida de uma ICP depende diretamente da forma como são tratadas a atualização e substituição dos certificados e chaves privadas de suas ACs. Para que esta forma seja alcançada, é necessário o desenvolvimento de métodos para que esta substituição seja executada conforme as necessidades específicas de cada ICP. O presente artigo apresenta possíveis tipos de substituições e seus respectivos procedimentos para que a gerência do ciclo de vida uma ICP seja feita da forma mais clara e completa.

Abstract

The best PKI life cycle management strategy depends directly on the strategy to deal with the update and replacement of CAs certificate and private key. To reach this best strategy, it is necessary to develop methods in which replacement is executed as the specific needs of each PKI. This article presents possible strategies for replacement, and corresponding procedures, so that the PKI life cycle management be conducted in the most clear and complete way.

1 Introdução

O uso em larga escala de chaves públicas para propiciar segurança às comunicações e transações eletrônicas em computadores só foi possível graças a estruturação de mecanismos criptográficos e de técnicas de gestão na forma de uma infra-estrutura de chaves públicas (ICP) e ao esforço da comunidade científica e de organizações empresariais na elaboração de normas e recomendações [1, 2] que regulamentam a forma adequada de se implementar uma ICP. Entretanto, constatou-se após duas décadas de uso, que estas normas são extremamente rígidas e não preveêm determinadas funcionalidades as quais dificultam a operação a longo prazo da ICP. Um desses problemas, o qual este artigo trata, consiste na substituição do certificado ou do par de chaves criptográficas da Autoridade Certificadora (AC).

As recomendações RFC 3280 [1] e RFC 4210 [2], preveêm apenas um caso para a substituição do par de chaves de uma AC. Este se refere a atualização deste quando o antigo par de chaves da AC está disponível. Entretanto, à medida em que os certificados digitais de AC reais começaram a expirar, constatou-se situações não previstas nestas normas. São os casos quando não se tem acesso

a chave privada anterior da AC ou quando não se pode realizar, por restrições do hardware, do protocolo de gestão de chaves ou da política, a cópia da chave privada antiga. Não há referências na literatura especializada, de mecanismos para tratar adequadamente estes problemas.

Em teoria, existem dois tipos de operações de substituição que podem ser realizadas sobre uma AC: a simples substituição do certificado digital mantendo a chave privada antiga ou a substituição com a troca da chave privada. A substituição da chave privada pode ainda ser realizada com ou sem a disponibilidade da chave privada antiga. E se disponível, pode ser com a possibilidade de sua cópia (backup) ou não.

Este artigo propõe novos métodos para para a substituição das chaves para cada uma destas situações.

A seção 2 detalha a situação prevista nas RFC. A seção 3 apresenta as técnicas de substituição do certificado e do par chaves de AC. A seção 4 detalha o procedimento de validação e testes da proposta. A seção 5 contém as considerações finais do artigo.

2 O modelo atual

Para apresentar um novo certificado digital ou uma nova chave de assinatura de listas de certificados revogados (LCR), uma AC deve emitir certificados de transição [2, 3, 4] para o antigo e novo par de chaves. Os certificados de transição são necessários para que os subscritores de certificados pertencentes a uma ICP possam construir um caminho de certificação válido para certificados pertencentes à mesma ICP, mas assinados com uma nova chave privada. O procedimento básico consiste em guarnecer a nova chave pública utilizando a antiga chave privada e vice-versa, conforme ilustra a Figura 1.

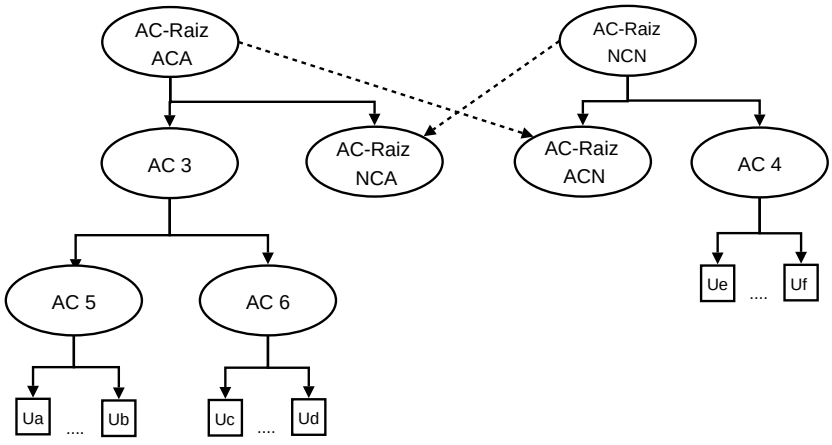

Figura 1: Estrutura hierárquica após troca do par de chaves da AC Raiz. As linhas tracejadas indicam que os certificados são semelhantes ao da origem e não uma hierarquia. ACN é a AC *Antiga-com-Nova*, NCA é a AC *Nova-com-Antiga*, ACA é a AC *Antiga-com-Antiga*, NCN é a AC *Nova-com-Nova*.

Para a realização deste processo, devem ser gerados 3 novos certificados: o certificado da nova AC Raiz e dois certificados de transição, um assinado

pela nova chave privada que contém a chave pública do certificado antigo e o outro assinado pela chave privada antiga que contém a chave pública do novo certificado.

Ao final do processo, existirão 4 certificados da mesma AC: o antigo (*Antigo-com-Antigo*); o novo (*Novo-com-Novo*); o antigo assinado com a nova chave privada (*Antigo-com-Novo*); e o novo assinado com a antiga chave privada (*Novo-com-Antigo*) [2].

O certificado *Antigo-com-Novo* (ACN) contém a chave pública do certificado antigo, e é assinado pela nova chave privada. Desta forma, é possível aos detentores de certificados assinados pela nova chave privada, a construção de um caminho de certificação válido para os certificados assinados com a chave privada antiga [3]. Para este certificado, o período de validade se inicia no momento em que o certificado é emitido e termina na mesma data que vence o certificado que contém a chave pública antiga [2]. A chave pública deste certificado é a mesma do certificado antigo.

O certificado *Novo-com-Antigo* (NCA) contém a chave pública do certificado novo, e é assinado pela chave privada antiga. Assim, os detentores de certificados assinados pela chave privada antiga podem construir um caminho de certificação válido para os certificados assinados com a nova chave privada [3]. O período de validade se inicia no momento em que o certificado é emitido e tem como data de validade o tempo necessário para que todas as entidades desta AC possuam a nova chave pública, no pior caso, a data de validade da chave pública antiga [2].

O certificado *Antigo-com-Antigo* (ACA) é o certificado original. O certificado *Novo-com-Novo* (NCN) é o certificado digital auto-assinado emitido para o novo par de chaves criptográficas.

3 A nova abordagem

O método descrito na Seção 2 descreve o procedimento a ser realizado quando há a necessidade de troca do par de chaves da AC Raiz [2]. Este método, embora bastante funcional, não possui toda a abrangência necessária de forma a cumprir todos os requisitos de uma ICP durante seu ciclo de vida. Seu objetivo é a simples substituição da chave privada da AC raiz. Nesta seção, será apresentado em detalhes um novo modelo que atende diversas outras situações de substituição da AC-Raiz. Como já discutido, existem dois tipos de operações que, se realizadas em uma AC, podem causar algum impacto em sua topologia, que são a substituição do certificado e a substituição da chave privada. Cada uma dessas alterações possui algumas subdivisões que necessitam ser tratadas de forma diferenciada. No decorrer desta seção, cada uma destas operações é descrita e uma respectiva solução é proposta.

3.1 Alteração do Certificado

Os certificados possuem um tempo de vida fixo quando são emitidos. Quando se aproxima da data final de validade, é necessária a emissão de um novo certificado [5] e, eventualmente, a geração de um novo par de chaves criptográficas. A alteração de um certificado de AC faz-se necessária por vários motivos. Além da questão do período de validade, pode existir a necessidade de alteração de

algum atributo, ou modificação de alguma política. Em todos estes casos, a substituição da chave privada não é necessária caso ela esteja disponível e não exista nenhuma restrição quando a sua segurança ou política. Este processo pode ser divido em dois tipos: o de alteração do certificado, que se aplica à necessidade de mudança em algum de seus atributos, e o de renovação, onde embora seja necessária a substituição do certificado, recomenda-se a manutenção de todos os seus atributos, com exceção das datas de início e fim de validade.

O processo de alteração é realizado a partir da criação de uma requisição [6] de certificado mantendo a mesma chave pública do certificado antigo. A partir desta requisição, é emitido um novo certificado com a mesma chave pública. Este procedimento pode ser aplicado de forma semelhante tanto para uma AC Raiz quanto para uma AC intermediária e até mesmo para certificados de entidades finais, diferindo apenas pelo fato de que para a AC Raiz, o novo certificado é auto-assinado, enquanto que para uma AC intermediária ou para a entidade final, o novo certificado é emitido pela mesma AC que emitiu o certificado antigo, passando pelo mesmo processo referente a emissão de um certificado normal.

O caso da renovação é ainda mais simples. Com os dados do certificado antigo, é gerada uma nova requisição com os mesmos dados, inclusive com a mesma chave pública. A partir desta requisição, é gerado um novo certificado. A diferença do certificado anterior para este novo certificado, é apenas nas datas de emissão e validade. Todos os outros valores são iguais. Para este caso, nada impede que seja implantado um sistema que faça isto de forma automática, e conseqüentemente, elimine a necessidade de uma nova verificação dos dados da requisição.

3.2 Substituição da chave privada

Quando existe a necessidade de substituição da chave privada de uma AC e a conseqüente troca de seu certificado, podem ocorrer dois casos: um quando a chave privada está disponível; e o outro quando a situação oposta ocorre, ou seja, não se tem acesso a chave. Cada um dos casos requer um tratamento específico e diferenciado com a finalidade de proporcionar o menor impacto possível para a topologia da ICP. A seguir será descrito como proceder na ocorrência de cada um destes casos.

3.2.1 Sem chave privada disponível

A conceito de disponibilidade é muito importante quando trata do acesso à chave privada de uma AC. Quando a chave privada não está disponível, seja devido a uma falha no dispositivo que a armazena ou até mesmo por restrições políticas ou físicas sobre seu uso, toda a estrutura é prejudicada. Até o presente momento, a única solução encontrada para este problema é a reemissão de todos os certificados emitidos pela AC e em todos os seus níveis inferiores de sua hierarquia. Tal aplicação pode ser viável e até rotineira em pequenos ambientes, para solucionar problemas como a necessidade de emissão de LCRs [7]. Porém, em ACs onde existe um grande número de certificados emitidos, ou em ACs que emitem certificados de ACs, este procedimento passa a ser inviável e de om custo muito elevado.

O modelo apresentado na Seção 2 não pode ser aplicado neste caso pelo fato da chave privada não estar disponível, e conseqüentemente a AC antiga não

poderá assinar o certificado de transição (*Novo-Com-Antigo*). Devido a isto, o procedimento de emissão do novo certificado será diferente do visto anteriormente.

Em uma ICP já estabelecida, como a da Figura 2, deve-se criar uma nova AC, que no exemplo da Figura 3, é chamada de AC-Raiz *NCN*. Esta nova AC possuirá um novo par de chaves, porém deve conter os mesmos dados do certificado da AC-Raiz ACA, diferindo apenas nas datas de emissão e validade, além da chave pública. A diferença na criação deste certificado em relação ao processo de renovação descrito na Seção 3.1 é que a chave contida na requisição é a nova chave pública, ao invés da utilização da antiga.

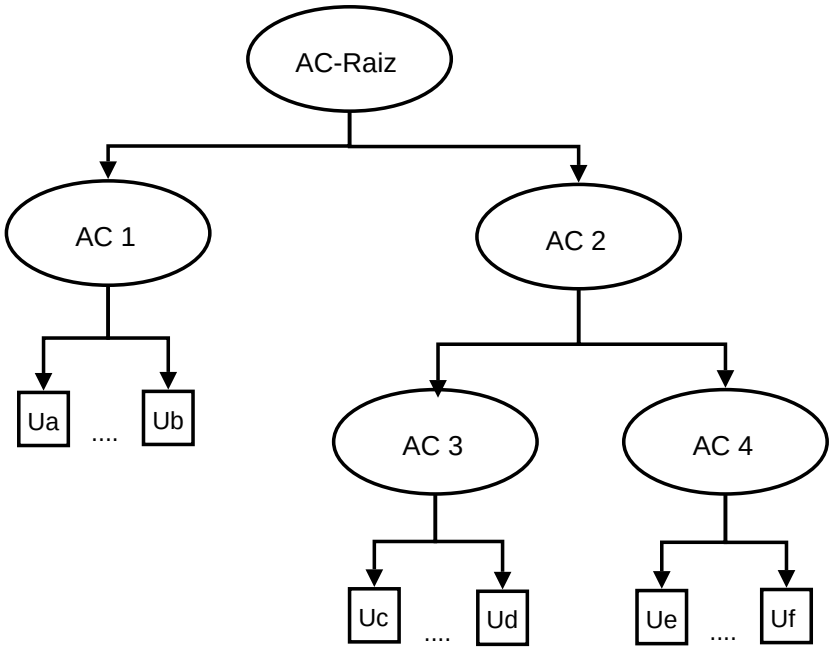

Figura 2: Estrutura de AC Hierárquica

Com a AC-Raiz *NCN* em funcionamento, o próximo passo é gerar requisições a partir de todos os certificados emitidos pela AC ACA, se estendendo apenas em um nível hierárquico. Novamente o processo é bastante semelhante ao de atualização definido na Seção 3.1. A única diferença é que estas requisições serão submetidas a nova AC, ou seja, a AC-Raiz *NCN*. Geradas as requisições, a AC-Raiz *NCN* emite os certificados referentes as requisições criadas. Após este passo, o processo referente a geração de requisições e emissão de certificados estará concluído.

Todos os certificados emitidos em níveis hierárquicos inferiores aos certificados reemitidos não sofrerão implicações, pois a chave privada utilizada em sua assinatura dos certificados será a mesma. Deve-se apenas publicar o novo certificado da AC-Raiz de forma que todos que necessitem obter este novo certificado possam fazê-lo. As novas ACs geradas no processo podem desempenhar o mesmo papel das ACs anteriores (emissão e revogação de certificados, criação de LCRs, etc). A Figura 4 apresenta a nova estrutura após toda a realização

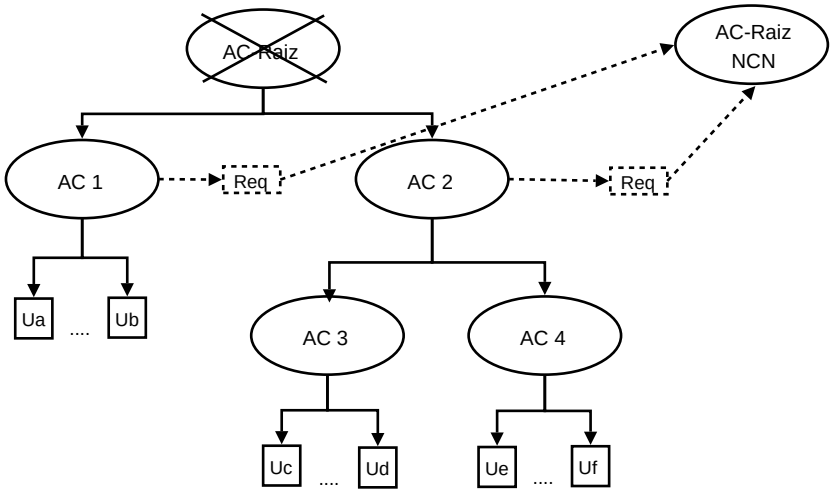

Figura 3: Pedidos de requisição para a nova AC

do processo.

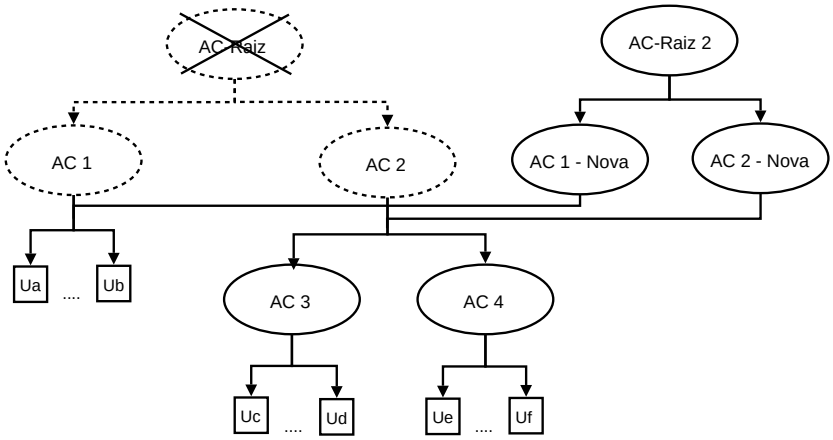

Figura 4: Nova estrutura hierárquica

Não existe nenhum impedimento técnico para que este procedimento seja executado em ACs intermediárias ao invés de ACs Raízes, porém se esta AC emite apenas certificados para entidades finais, o custo será o mesmo da reemissão de todos os certificados já emitidos.

3.2.2 Com chave privada disponível

Quando se tem a chave privada disponível e deseja-se realizar a troca da chave privada, existem dois casos que podem ser diferenciados. Um onde quando existe a disponibilidade da chave privada e há formas de realização de cópia das chaves e outra onde não há forma de que isso se realize, ou seja, a chave estará acessível, porém não há meios de realizar sua cópia.

Com a possibilidade de cópia da chave

Caso a chave privada esteja disponível e existam restrições quanto a realização de sua cópia, pode-se considerar que a chave privada está realmente protegida e sem chances de perda. Desta forma, o procedimento descrito na RFC 4210 pode ser utilizado sem problemas.

Vale lembrar que este processo, embora trate apenas do uso em AC-Raiz, pode ser utilizado também em ACs intermediárias.

Sem a possibilidade de cópia da chave

Quando a chave privada, por restrições legais, políticas, de software ou hardware não pode ser copiada, existe um ponto importante a ser levado em consideração. Trata-se da confiança na entidade que armazena a chave. Uma vez que ocorra qualquer problema, a chave privada será perdida e não haverá forma de recuperá-la. Neste caso, pode-se adotar duas soluções: a aplicação do procedimento apresentado na RFC 4210 para criar uma nova AC em ambiente de maior confiabilidade; ou continuar a utilização do sistema e caso ocorra algum problema, realizar o procedimento descrito na Seção 3.2.1. Neste segundo caso, se houver a necessidade de atualização apenas do certificado, pode-se utilizar o processo descrito na Seção 3.1, porém os riscos de perda da chave permenecem altos devido as suas restrições de cópia.

4 Resultados obtidos

Para a validação e testes da proposta, foi implementada uma solução baseada na utilização do OpenSSL [8] em um sistema operacional Linux. Foi criada a ICP apresentada na Figura 5 e para todos os métodos descritos nas seção anteriores foi utilizada esta estrutura.

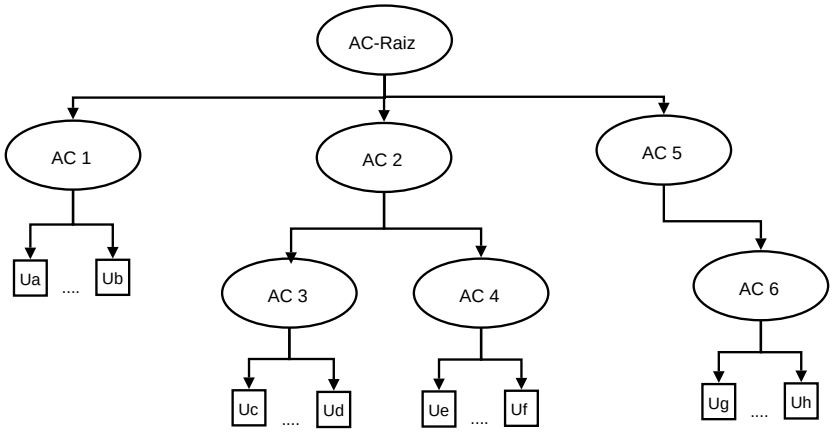

Figura 5: Estrutura hierárquica para Validação e Testes das Propostas.

4.1 Alteração do certificado

O procedimento para a implementação do processo descrito na Seção 3.1 deste artigo foi realizado da seguinte forma:

- a estrutura foi criada buscando reproduzir uma estrutura hierárquica comum de uma AC;
- foi emitida uma série de certificados finais a partir de todas as ACs do caminho de certificação;
- a partir dos dados do certificado da AC-Raiz foi gerada uma nova requisição utilizando a mesma chave pública;
- a partir da requisição gerada foi criado um novo certificado de AC Raiz;
- foram realizados testes de montagem e verificação do caminho de certificação.

A verificação da montagem e validação do caminho de certificação foi realizada utilizando o Openssl e os browsers Firefox e Internet Explorer. Em todos os casos, a cadeia foi montada corretamente a partir do momento em que foi adicionado o novo certificado da AC-Raiz na lista dos certificados confiáveis. Desta forma, pôde-se verificar que a utilização do mecanismo é viável.

O impacto da aplicação desta técnica sobre o restante da ICP pode ser considerado nulo quando se leva em consideração a montagem do caminho de certificação e sua verificação, uma vez que o par de chaves é o mesmo.

4.2 Substituição da chave privada

O procedimento para a implementação do processo descrito na Seção 3.2.1 deste artigo foi realizado da seguinte forma:

- a estrutura foi criada buscando reproduzir uma estrutura hierárquica comum de uma AC;
- foram emitidos certificados finais a partir de todas as ACs do caminho de certificação;
- a chave da AC-Raiz foi destruída;
- criou-se uma nova AC-Raiz, chamada AC-Raiz *NCN*;
- a partir dos certificados que estão um nível abaixo da AC Raiz, foram emitidas requisições, mantendo sempre os mesmos dados e o mesmo par de chaves;
- A AC Raiz *NCN* emitiu todos os certificados a partir das requisições.

A verificação da montagem correta do caminho de certificação foi realizada utilizando o Openssl e os browsers Firefox e Internet Explorer. Em todos os casos, a cadeia foi montada corretamente a partir do momento em que foi adicionado o novo certificado da AC-Raiz na lista dos certificados confiáveis.

Analisando a redução do impacto em relação a reemissão de todos os certificados, pode-se dizer que este foi mínimo, já que a necessidade de reemissão de certificados se restringiu a um único nível na cadeia de certificação. Uma AC-Raiz com 10 certificados de ACs intermediárias, e cada uma destas ACs com 1000 certificados emitidos, a aplicação deste método reduziria a necessidade de

reemissão de 10010 para 10 certificados. Ou seja, o número de certificados a serem reemitidos com a utilizacão deste método é igual ao número de certificados emitidos pela AC-Raiz, excluindo-se quaisquer outros certificados emitidos por suas ACs intermediárias.

Já no caso da aplicação desta técnica em uma AC intermediária, o impacto pode ser maior. Isto depende se a AC emite certificados para entidades finais ou para outras ACs.

5 Conclusões

Foram discutidas as várias possibilidades e necessidades de substituição do certificado de uma AC Raiz ou de sua chave privada. Para cada uma destas possibilidades, foi proposto um mecanismo eficiente para realizar a substituição desejada.

Para o caso da alteração do certificado, mostrou-se que a partir do certificado antigo é possível realizar sua renovação ou alteração de maneira simples, sem que a topologia da ICP seja afetada. Além disso, mostrou-se viável a implantação de um sistema para a automatização deste processo.

No caso da substituição da chave privada, viu-se que a diferenciação do procedimento de substituição a partir da disponibilidade da chave privada, faz com que o impacto deste processo seja menor do que em um procedimento genérico, além disso, torna possível a solução eficiente de situações não previstas pelas normas.

A partir da implementação de um protótipo para validação e testes das propostas, foi possível provar que além de funcionais, as técnicas apresentadas são aplicáveis na prática.

Referências

[1] HOUSLEY, R. et al. Certificate and certificate revocation list profile. Abril 2002. Disponível em: <http://www.ietf.org/rfc/rfc3280.txt>.

[2] ADAMS, C. et al. Internet x.509 public key infrastructure certificate management protocol. Março 1999. Disponível em: <http://www.ietf.org/rfc/rfc4210.txt>.

[3] HOUSLEY, R.; POLK, T. *Planning for PKI*. 1. ed. [S.l.]: Wiley, 2001.

[4] JEUN, I. et al. A best practice for root ca key update in pki. In: *ACNS*. [S.l.: s.n.], 2004. p. 278–291.

[5] ADAMS, C.; LLOYD, S. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. 2. ed. [S.l.]: Addison Wesley, 2002. 352 p.

[6] MYERS, M. et al. Certificate request message format. Setembro 2005. Disponível em: <http://www.ietf.org/rfc/rfc2511.txt>.

[7] HSU, Y.-K.; SEYMOUR, S. P. An intranet security framework based on short-lived certificates. *IEEE Internet Computing*, 1998.

[8] OPENSSL. Disponível em: <http://www.openssl.org>.