Sistema Gerenciador de Certificados Digitais: Um modelo para governo eletrônico

Lucas Gonçalves Martins[1], **Ricardo Felipe Custódio**[1]

[1]Departamento de Informática e Estatística
Universidade Federal de Santa Catarina (UFSC)
Florianópolis – SC – Brasil

{lucasgm,custodio}@inf.ufsc.br

Resumo. *Esse artigo propõe um modelo de sistemas gerenciadores de certificados digitais para infraestruturas de chave públicas governamentais. O modelo define módulos independentes que podem ser configurados para obter eficiência, performance, redundância e distribuição geográfica das funções de autoridades certificadoras e registradoras, de forma escalável, com controle e auditoria centralizados.*

Abstract. *This paper proposes a model for certificate management systems for e-governments. The model defines independent modules that can be configured to achieve improved efficiency, performance, redundancy and geographical distribution of certification and registration authorities functions, with a centralized auditing.*

1. Introdução

O uso de tecnologia - para automação, integração e redução de custos - está aproximando vários governos do mundo digital. O termo governo eletrônico (*e-government*) tem sido usado para definir os países que usam tecnologia para beneficiarem seus sistemas de governo [Layne and Lee 2001]. Um dos maiores desafios do governo eletrônico é definir um método para identificar e autenticar legalmente seus cidadãos [New Zeland 2011].

A infraestrutura de chaves públicas (ICP) é uma das soluções mais próxima da legalização da identidade eletrônica. Uma ICP é usada para criar evidências que dão credibilidade a certificados digitais. Mas, a confiança sobre o certificado é dada pelo o seu usuário. Ele é responsável por decidir se a ICP, onde o certificado está inserido, é confiável o suficiente para o contexto em que ele o está usando. Por outro lado, a legalidade de uma ICP não depende dos seus usuários. É responsabilidade do governo estabelecer as regras que dão valor legal a uma ICP em seu território. Alguns países estabelecem ICPs governamentais, onde a autoridade certificadora (AC) raiz é controlada por uma entidade do governo. Assim, o governo consegue controlar quais entidades podem se juntar à ICP e quais políticas essas entidades devem seguir. Porém, uma ICP governamental costuma ser maior e mais complexa do que uma privada, além de estar diretamente ligada a soberania de seu país, já que é dada fé pública aos seus certificados digitais.

O gerenciamento de certificados digitais é feito através de um conjunto de dispositivos, aplicações e pessoas, chamado de sistema gerenciador de certificados (SGC) [Housley and Polk 2001]. Normalmente, cada autoridade certificadora utiliza seu próprio

SGC, desde que o mesmo se encontre dentro dos conformes esperados pela ICP. Porém, a variedade de soluções de SGC em uma ICP pode acarretar em problemas de compatibilidade e segurança, devido a complexidade dos processos de homologação. Além disso, apesar de na literatura existirem diversos padrões para a certificação digital, existem poucas referências de modelos completos para sistemas gerenciadores de certificados. Países interessados em estabelecer regras de implementação para esses sistemas, precisam criar projetos para construir seus próprios modelos de SGC.

Este artigo propõe um modelo de sistemas gerenciadores de certificado para governos eletrônicos. Ele define componentes de alta coesão e baixo acoplamento, compatíveis com balanceamento de carga, distribuição geográfica e redundância contra falhas, sendo todas essas características facilmente escaláveis. O modelo ainda garante controle e auditoria centralizados das ACs e ARS.

Todo o modelo segue as especificações da RFC-5280 e é compatível com os protocolos mais usados para gerenciamento de certificados digitais, como o *Certificate Management over CMS* (CMC) e *Certificate Management Protocol* (CMP). Porém, este trabalho se limita a especificar as principais funções de AC e AR. Tecnologias como LDAP, OCSP, balanceamento de carga e redundância não são especificados. Nós assumimos que através de nosso modelo é possível aplicar métodos já existentes para esses fins.

Organização do Artigo O restante deste artigo está organizado em cinco seções. Na seção 2 listamos e discutimos alguns dos trabalhos relacionados à esse artigo. Na seção 3 damos a especificação do nosso modelo e suas funções. Na seção 4 falamos sobre as tecnologias usadas na implementação de um protótipo do modelo. Na seçao 5 fazemos uma analise do nosso modelo e comparações com SGCs existentes. Por fim, na seção 6 damos nossas considerações finais e listamos alguns dos trabalhos futuros.

2. Trabalhos Relacionados

Padrões em ICP. Hoje, a padronização da certificação digital é feita, principalmente, pela *Internet Engineering Task Force* (IETF) no formato de *Requests For Comments* (RFC). Esses padrões cobrem a especificação de estruturas, protocolos, políticas e infraestruturas, que são implementadas pela maior parte das aplicações compatíveis com ICP. A RFC 5280 - *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [Cooper et al. 2008] define as estruturas de dados para certificados digitais e lista de certificados revogados, bem como as regras de preenchimento e interpretação dessas estruturas. A RFC também especifica um algoritmo para a construção e validação de caminhos de certificação.

As RFCs 4210 [Adams et al. 2005] e 5272 [Schaad and Myers 2008] especificam protocolos de gerenciamento de certificados digitais e definem um modelo mais elaborado de distribuição das funções da ICP. Além das RFCs existem outras fontes de padronização para ICP, como o PKCS (*Public-key Cryptography Standards*), a iso ISO/IEC 9594-8/ITU-T X.509 e recomendações de instituições como NSA (*National Security Agency*) e a *RSA Laboratories*.

ICP-Brasil. Desde 2001, quando a ICP-Brasil foi legalizada pela medida provisória 2002-2 [Brazil 2001], o governo brasileiro vêm investindo na sua ICP governamental. Vários documentos foram escritos para definir os padrões que deveriam ser seguidos pelas entidades e aplicações da ICP-Brasil. Dentre esses documentos, exitem dois volumes

do *Manual de Conduta Técnica 11* [ITI 2010b, ITI 2010a], que especificam requisitos mínimos, recomendações e procedimentos de validação para sistema gerenciadores de certificados das ACs e ARs da ICP-Brasil. Esses documento foram embasado em RFCs, PKCS (*Public-key Cryptography Standards*) e outros documentos da própria ICP-Brasil. Tendo conhecimento de que esses padrões não definem requisitos de software, deduzimos que a escrita desse manual exigiu uma equipe de pesquisa para criar o modelo de SGC.

EJBCA Enterprise PKI. O EJBCA Enterprise PKI [PrimeKey Solutions 2013] é uma implementação robusta de SGC em código aberto. Ele implementa tanto as funçõs de AC como de AR e é compatível como o protocolo CMP para gerenciamento de certificados digitais. Além de AC e AR, ele também define um módulo de autoridade de validação, responsável por atender as consultas OCSP e LDAP da AC. Através de uma intância do EJBCA, é possível criar e gerenciar diversas ACs. Porém, o módulo de AR é o mesmo para todas elas e se encontra na mesma instância do EJBCA. Para a integração com ARs externas, é fornecida uma API de AR, que acessa diretamente dados de um banco de dados de uma AR que se encontra em uma outra instância fora dos limites da instalação da AC.

3. Sistema Gerenciador de Certificados

Antes de apresentarmos a especificação do nosso modelo, nós damos uma breve introdução sobre autoridades certificadoras e registradoras. A figura 1 ilustra um diagrama dessas entidades e suas relações com usuários finais e agentes de registro. Nela, a entidade *AC* representa um conjunto de autoridades certificadoras, entidades responsáveis por inserir (emitir) e remover (revogar) certificado digitais da cadeia de certificação da ICP. A entidade *AR* representa um conjunto de autoridades registradoras, entidades especializadas na identificação e autenticação de outras entidades, como pessoas, empresas e máquinas. A entidade *Usuário* representa as pessoas que desejam obter um certificado digital, enquanto a entidade *AGR* representa os empregados das ARs.

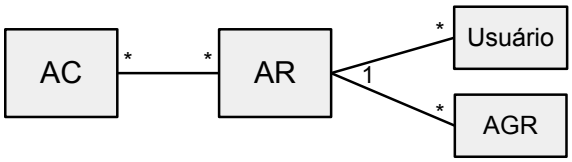

Figura 1. Diagrama Relacional AC-AR

A relação entre AC e AR indica um vínculo de confiança entre essas entidades. Esse vínculo delega os serviços de relação com o usuário da AC para a AR. Por exemplo, antes de emitir um certificado digital, a AC precisa identificar e autenticar o requerente. Caso a AC tenha um vínculo com uma AR, essa AR fica responsável por realizar essa verificação e autorizar a emissão do certificado digital. Dessa forma, a AC precisa apenas se comunicar com a AR, evitando o uso de um canal público ente a aplicação da AC e seus usuário.

Os métodos de autenticação usados pela AR depende do seu contexto. As vezes, uma simples verificação de posse de email é suficiente. Porém, no contexto de um governo eletrônico é necessário que a AR faça verificações face-a-face de documento oficiais do país. Nesses casos, a AR precisa de empregados para realizar essas verificações,

conhecidos por agentes de registro (AGR). Esses empregados costumam trabalhar em instalações técnicas (IT), onde possuem máquinas autorizadas a acessar as funções da AR. Além disso, para permitir que o usuário tenha fácil acesso aos agentes de registro, as ARs podem espalhar instalações técnicas na área geográfica em que atende esses usuários.

3.1. Visão Geral do Modelo

Nosso modelo para sistemas gerenciadores de certificados é dividido em dois subsistemas. Um para autoridades certificadoras e outro par autoridades registradoras. Na figura 2, esses sistemas são representados pelos ambientes de AC e de AR, respectivamente. Cada um dos ambientes é dividido em módulos servidores e módulos gerenciadores, chamados: Servidor de AC (SAC), Servidor de AR (SAR), Sistema Gerenciador de AC (SGAC) e Sistema Gerenciador de AR (SGAR).

Cada ambiente também possui um banco de dados, compartilhado entre seus respectivos módulos servidores e gerenciadores. Esse banco de dados pode ser interpretado de forma genérica, desde que ele possua uma interface padronizada de acesso aos dados armazenados. Nele encontram-se instâncias de base de dados, para cada autoridade certificadora e registradora instanciada no SGC. Sendo que as instâncias de base de dados são acessíveis apenas pelos módulos relacionados à AC ou AR em questão. Apesar do projeto possuir uma solução detalhada para o banco de dados de ACs e ARs, não aprofundamos esse tema neste artigo.

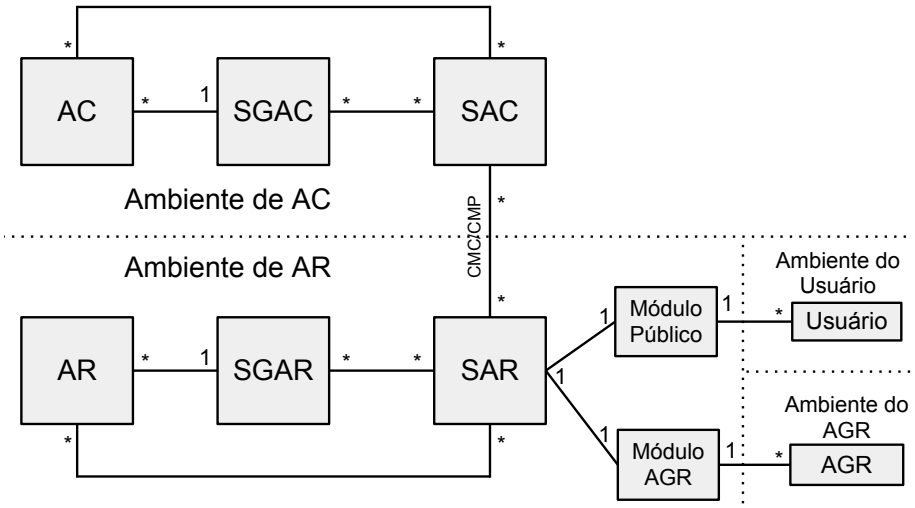

Figura 2. Diagrama Relacional Completo do Modelo

O ambiente de AC é composto por um SGAC, um conjunto de SACs, um banco de dados e um módulo de segurança criptográfico (MSC). O SGAC é responsável pela criação, configuração e auditoria de ACs. Através de uma instância dele é possível gerenciar mais de uma AC, sendo que para cada uma delas, uma base de dados é criada separadamente. O SGAC também é responsável pela criação das chaves criptográficas da AC (no MSC) e por autorizar servidores a acessarem essas chaves e ao banco de dados da AC. O O SAC executa as funções de AC, funcionando automaticamente através do protocolo de gerenciamento de certificados escolhido. Para isso, ele precisa ter sido autorizado, por um SGAC, à acessar o banco de dados e chaves da AC.

O ambiente de AR é similar ao ambiente de AC. Ele é composto por um SGAR, um conjunto de SARs, um banco de dados e um módulos de segurança criptográfico. O SGAR funciona da mesma forma que o SGAC, sendo que ele possui funções de cadastramento de AGR e instalações técnicas. A maior diferença do ambiente de AR se encontra em seus servidores (SAR), que operam em três frentes diferentes: com os servidores de AC, com os agentes de registro e com os usuário finais. A comunicação com a AC funciona automaticamente, através de um protocolo de gerenciamento de certificado. A comunicação com usuários e AGRs ocorrem através de aplicações remotas, conhecidas como módulo público e módulo de agente de registro, respectivamente.

O ambiente de AGR é uma instalação técnica, onde o agente de registro possui uma máquina autorizada a acessar o módulo de agente de registro. Através dessa máquina ele é capaz de buscar, aprovar e rejeitar solicitações de emissão e revogação de certificados digitais. O ambiente do usuário final é uma máquina pessoal, na qual o usuário confia e usa para acessar o módulo público. Através dela, o usuário é capaz de fazer solicitações de emissão e revogação de certificados digitais, além de gerar chaves criptográficas e assinar requisições de certificados.

Na figura 2 a relação entre *SGAC* e *AC* indica as ACs gerenciadas pelo SGAC. Essa relação é de um para muitos, fazendo com que um SGAC possa gerenciar várias ACs, mas uma AC só possa ser gerenciada por um SGAC. A relação entre SGAC e SAC indica os servidores usados pelo SGAC para operar suas ACs. Essa relação é de muitos para muitos, indicando que um SGAC pode utilizar vários SACs e um SAC pode ser usado por vários SGACs. A relação entre SAC e AC indica em quais servidores cada AC está sendo executada. Essa relação também é de muitos para muitos, indicando que uma AC pode estar sendo executada ao mesmo tempo em diversos servidores e que um servidor pode estar operando mais de uma AC por vez. Todas essas relações tem o mesmo sentido no ambiente de AR.

A relação entre AC e AR tem o mesmo sentido da relação entre essas entidades ilustrada na figura 1. A relação entre SAC e RAS indica que esses servidores operam pelo menos uma AC e uma AR, respectivamente, que possuem uma relação de confiança. Essa relação também representa o canal de comunicação para os protocolos de gerenciamento de certificados, usados na comunicação entre AC e AR. A relação entre SAR e os módulos público e de agente de registro indica o canal de comunicação da AR com os usuário e agentes de registro. Esse canal também pode ser usado para troca de mensagens do protocolo de gerenciamento de certificado usado.

3.2. Distribuição de Servidores

Nosso modelo é maleável e pode ter seus módulos configurados de diversas formas diferentes. Nós mostramos na figura 3 três exemplos de configuração para explicar como elas podem ser usadas para garantir balanceamento de carga, distribuição geográfica, redundância e eficiência, de forma escalável. Em todos exemplos nós usamos um ambiente de AC, porém todas as configurações podem ser usadas em um ambiente de AR. Cada uma das configurações possui duas autoridades certificadoras gerenciadas por um Gerenciador de AC. A diferença entre elas se encontra na forma que as ACs são distribuídas entre os módulos servidores.

A primeira configuração (esquerda) ilustra um SGAC que distribui cada uma de

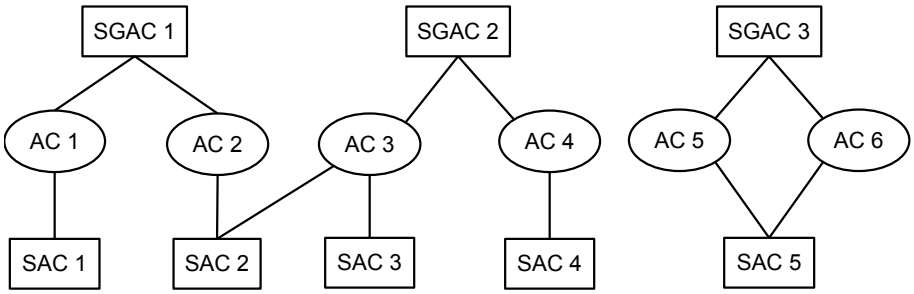

Figura 3. Exemplos de Configuração dos Módulos

suas ACs em servidores diferentes. Esse tipo de configuração é útil para ICPs que distribuem diversas ACs em uma grande área geográfica, mas que ao mesmo tempo precisam manter um controle centralizado de todas elas. Como, por exemplo, um país que estabelece que cada um dos seus estados deve possuir sua própria AC, mas que elas devem ser controladas e auditadas de um ponto central. Fazemos isso mantendo todas as ACs em um SGAC e distribuindo os servidores das ACs nas áreas em que elas vão atuar.

A terceira configuração (direita) mostra um SGAC que disponibilizas suas ACs em apenas um servidor (SAC 5). Esse tipo de configuração garante uma melhor eficiência, pois usa menos recursos (SAC) para manter mais de uma AC online. Entidades que controlam muitas ACs, mas possuem poucos usuários, podem usar essa configuração pela sua simplicidade e custo reduzido. Como, por exemplo, o governo de um estado que deseja separar em ACs diferentes a emissão de certificados para cidadãos e para empresas. Sendo um servidor capaz de atender toda a população desse estado, basta centralizar suas ACs em um único servidor, economizando recursos da ICP.

A segunda configuração (centro) mostra uma configuração hibrida. Ela possui uma de suas ACs em um servidor dedicado e a outra em dois servidores diferentes, sendo um servidor compartilhado com uma AC do SGAC 1. A distribuição de uma AC em mais de uma servidor permite que esses servidores sejam configurados em um equipamento de balanceamento de carga ou de redundância contra falhas, garantindo performance e disponibilidade para as funções da AC. Outro uso de múltiplos servidores é nos casos onde a distância geográfica pode prejudicar a qualidade do serviço. Através dessa configuração, é possível distribuir servidores da mesma AC em uma grande área geográfica.

Todas essas configuração são escaláveis. Conforme a demanda das ACs aumenta, ou novas ACs são criadas, novos servidores podem ser instalados. É apenas necessário que o SGAC, responsável pela AC, dê aos novos servidores acesso a base de dados da AC e suas chaves criptográficas.

4. Implementação

Para testar e avaliar nosso modelo, nós implementamos um protótipo de quatro aplicações. Os módulos gerenciadores (SGAC e SGAR) foram implementados na linguagem C++, enquanto os módulos servidores foram implementados em Java Web, sobre o servidor de aplicação *GlassFish*. Para a base de dados, usamos o SGbD MySQL. Para as funções criptográficas nós usamos a *libcrypto* em C++ do OpenSSL, e a biblioteca em Java *Bouncy Castle*. Como protocolo de gerenciamento de certificados, escolhemos o CMC, por sua simplicidade em comparação com o CMP. Como meio de transporte das mensagens do

protocolo, utilizamos a biblioteca para serviços web, *Jersey*. Como meio de comunicação com o módulo de segurança criptográfico, usamos a API *OpenSSL Engine*. Para o compartilhamento de chaves[1] criptográficas entre os módulos nós usamos um MSC com uma interface de rede, e segurança reduzida. Com a versão inicial do protótipo, conseguimos reproduzir todas configurações propostas, com exceção do uso de vários servidores para uma AC. Com essas configurações, simulamos as cerimônias de criação de AC, criação de AR, criação de vínculo entre AC e AR, cadastramento de servidores, emissão e revogação de certificados digitais, e emissão de LCR (manual e automática).

5. Discussão

Sistemas gerenciadores de certificados existentes no mercado, como o EJBCA [PrimeKey Solutions 2013], permitem a criação de diversas ACs em uma única instância e provém mecanismos de balanceamento de carga, redundância e distribuição geográfica. Porém, muitos desses mecanismos são funcionalidades da tecnologia utilizada por baixo do sistema. Normalmente, pelo servidor de aplicação. Essa tecnologia está fora do controle do governo, possui um nível elevado de complexidade e não está preparada para os requisitos de segurança de uma AC. Outro problema com as soluções existentes de SGC é a visão comercial sobre as ACs, ela faz com que essas soluções tenham os seus módulos de AR acoplados aos módulos de AC, já que ACs privadas não costumam prover serviços para ACs de outras empresas. Isso dificulta e até impede que as ARs desses sistemas prestem serviços para ACs de outra implementação.

Nosso modelo dá uma visão clara e separada dos sistemas de AC e AR, permitindo que essas entidades se comuniquem livremente. Além disso, o modelo separa, dentro do contexto individual de AC e AR, módulos de gerenciamento e de serviço. Os módulos de gerenciamento não são definidos em nenhum padrão, mas são úteis pois centralizam as cerimônias de criação, configuração, controle e auditora em um único ponto. Essa centralização, no contexto de governo eletrônico, é muito importante, pois permite que o governo organize suas ACs em pontos centralizados de controle. Além disso, a separação das funções de AC e AR em servidores independentes do módulo gerenciador, permite que padronizemos a tecnologia usada nesses servidores, criando sistemas embarcados ou *appliances* dedicados, da mesma forma que é feito com as urnas eletrônicas brasileiras. A padronização da tecnologia facilita a instalação da solução, reduz custos, garante total compatibilidade entre aplicações e facilita a homologação do sistema.

Outro ponto positivo do nosso modelo é a definição clara do módulo de agente de registro. No modelo previsto pelo *X.509*, apenas o usuário final se comunica com a AR. No nosso modelo, nós prevemos que a AR também provê um canal de comunicação específico para seus funcionários. Através desse canal, os AGRs são capazes de gerenciar as solicitações feitas pelos usuários finais. Porém, as mensagens que transitam por esse canal não são padronizadas por nenhum documento, fazendo com que cada AR gerencia da forma que achar melhor suas requisições. No contexto de governos eletrônicos, esse gerenciamento precisa ser padronizado.

6. Considerações Finais

Este trabalho faz parte de um esforço maior de especificação de sistemas gerenciadores de certificados para infraestrutura de chaves públicas governamentais. A complexidade desse projeto não permitiu que todo material de pesquisa fosse relatado neste artigo.

Porém, consideramos que atingimos nossos objetivos, que eram: apresentar o modelo; demonstrar as diversas configurações possíveis, com exemplos de uso em cenários reais, e; demonstrar as vantagens sobre modelos existentes de SGC.

O estágio de desenvolvimento desse modelo já se encontra bem avançado, com a padronização das base de dados de AC e AR e das cerimônias de emissão e revogação de certificados digitais. Para a conclusão do modelo, ainda faltam: (i) a definição das interfaces de acesso padronizado às informações de AC e AR; (ii) A modelagem de um *front-end* para compartilhamento de chaves criptográficas em módulos de segurança criptográficos; (iii) a definição dos protocolos de comunicação entre os módulos gerenciadores e servidores, e; (iv) a padronização das mensagens trocadas entre agente de registro e AR. Ao fim do projeto, desejamos entregar um modelo de SGC seguro, para ICPs governamentais, compatível com tecnologias de computação na nuvem, levando a certificação digital ao nível atual de tecnologia da computação.

Referências

Adams, C., Farrell, S., Kause, T., and Mononen, T. (2005). Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP). RFC 4210 (Proposed Standard).

Brazil (2001). Medida provisória no 2.200-2. Retrieved from: `http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm`.

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).

Housley, R. and Polk, T. (2001). *Planning for PKI: best practices guide for deploying public key infrastructure*. John Wiley & Sons, Inc.

ITI (2010a). *Manual de Condutas Técnicas 11 - Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Softwares de AC e AR no âmbito da ICP-Brasil*. Instituto Nacional de Tecnologia da Informação. Retrieved from: `http://www.iti.gov.br/index.php/icp-brasil/legislacao`.

ITI (2010b). *Manual de Condutas Técnicas 11 - Requisitos, Materiais e Documentos Técnicos para Homologação de Software de Autoridade Certificadora (AC) e Autoridade de Registro (AR) no Âmbito da ICP-Brasil*. Instituto Nacional de Tecnologia da Informação. Retrieved from: `http://www.iti.gov.br/index.php/icp-brasil/legislacao`.

Layne, K. and Lee, J. (2001). Developing fully functional E-government : A four stage model. volume 18, pages 122–136.

New Zeland (2011). E-government in New Zealand. Retrieved from: `<http://archive.ict.govt.nz/plone/archive/>`.

PrimeKey Solutions (2013). Ejbca enterprise pki. Retrieved from: `http://ejbca.sourceforge.net/`.

Schaad, J. and Myers, M. (2008). Certificate Management over CMS (CMC). RFC 5272 (Proposed Standard).