UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Gabriel Gaspar Becker

HAWA - SISTEMA GERENCIADOR DE CERTIFICADOS DIGITAIS ONLINE

Florianópolis

2013

Gabriel Gaspar Becker

HAWA - SISTEMA GERENCIADOR DE CERTIFICADOS DIGITAIS ONLINE

Monografia submetida à Ciências da Computação para a obtenção do Grau de Bacharelado em Ciências da Computação.
Orientador: Lucas Gonçalves Martins
Coorientador: Prof. Dr. Ricardo Felipe Cústodio

Florianópolis

2013

Gabriel Gaspar Becker

HAWA - SISTEMA GERENCIADOR DE CERTIFICADOS DIGITAIS ONLINE

Esta Monografia foi julgada aprovada para a obtenção do Título de "Bacharelado em Ciências da Computação", e aprovada em sua forma final pela Ciências da Computação.

Florianópolis, 01 de novembro 2013.

Prof. Chefe, Dr. Vitório Bruno Mazzola
Coordenador do Curso

Banca Examinadora:

Cristian Thiago Moecke

Marcelo Carlomagno Carlos

RESUMO

O presente trabalho apresenta o Sistema Gerenciador de Certificados Digitais Online e o panorama sobre a Infraestrutura de Chaves Públicas no Brasil e suas especificidades. Está subdividido em cinco capítulos: Introdução, Infraestrutura de Chaves Públicas, Sistema Gerenciador de Certificados Offline, Hawa - Sistema Gerenciador de Certificados Digitais Online e por fim as Considerações Finais. Este estudo apresenta o desenvolvimento do sistema de administração de um Sistema Gerenciador de Certificados Digitais Online, para tanto foram analisados os principais requisitos desse sistema, gerando um protótipo usável para realizar testes. A fundamentação teórica explicita os principais conceitos de Infraestrutura de Chaves Públicas. Os sistemas Ywapa e Ywyra foram avaliados e serviram como base para o desenvolvimento do sistema proposto. O objetivo do trabalho é desenvolver o Sistema Administrador de Autoridade Certificadora e o Sistema Administrador de Autoridade Registradora. As principais funções implementadas são: Gerenciar Servidores, Gerenciar Agentes de Registro, Gerenciar Instalações Técnicas e Gerenciar Vínculos de Confiança.

Palavras-chave: Sistema Gerenciador de Certificados Digitais Online, Infraestrutura de Chaves Públicas, Autoridade Certificadora, Autoridade Registradora, Certificado Digital, Assinatura Digital, Criptografia.

ABSTRACT

This paper introduces the Digital Certificate Management Online System and the overview of the Public Kye Infrastructure in Brazil and its specificities . Is divided into five chapters : Introduction , Public Key Infrastructure , Digital Certificate Management Offline System, Hawa - Digital Certificate Management Online System and at the end Concluding Remarks. This study presents the development of the administration system of a Digital Certificate Management Online System, for both were analyzed the main requirements of this system , generating a usable prototype to perform tests. The theoretical foundation explains the main concepts of Public Key Infrastructure . The Ywapa and Ywyra systems were evaluated and served as the basis for the development of the proposed system. The objective of work is to develop the Certification Authority Administration SystemSystem Certification Authority Administrator and Registration Authority Administration System. The main functions are implemented Manage Servers , Manage Registration Authority Officer , Manage Technical Instalations and Manage Trusted Authorities.

Keywords: Digital Certificate Management Online System, Public Key Infrastructure, Certification Authority, Registration Authority, Digital Certificate, Digital Signature, Criptography.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

SUMÁRIO

1 INTRODUÇÃO

A certificação digital fará parte do cotidiano de muitas pessoas, um exemplo disso é o Registro de Identidade Civil[1] (RIC), um projeto para a nova cédula de identidade no Brasil. Nesse projeto, cada cidadão portará um cartão que reunirá diversas informações de identificação, como o Cadastro de Pessoa Física (CPF), Título de Eleitor e o Registro Geral (RG). Nesse cartão também estará presente um certificado digital, que poderá ser usado para realizar diversas tarefas como assinar documentos digitais, declarar imposto de renda, registrar escrituras públicas, entre outras. Os certificados digitais embutidos no RIC serão emitidos e expedidos pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), válidos em todo o território nacional.

Não somente haverá um crescimento na demanda de certificação digital mas como já é realidade em muitos contextos. Como podemos perceber nas estatísticas fornecidas em [2] , mais de dois milhões de certificados digitais já foram emitidos e estão em uso no Brasil.

A ICP-Brasil foi instituída em agosto de 2001, como consta na medida provisória de número 2.002-2[3] , e regulamenta a certificação digital no Brasil. De acordo com a medida, o Instituto Nacional de Tecnologia (ITI) foi transformado em uma autarquia[4] .

Em 2003 a ICP-Brasil lançou um projeto intitulado: Programa João de Barro[5] , que teve como propósito inicial desenvolver uma nova plataforma criptográfica para a Autoridade Certificadora (AC) Raiz da ICP-Brasil. Essa plataforma é composta por hardware e software. O software produzido foi chamado de Ywapa e tinha por objetivo emitir o certificado da Autoridade Certificadora Raiz (AC Raiz) e gerenciar o ciclo de vida das ACs de primeiro nível. O hardware ainda está em processo de desenvolvimento e para a geração do par de chaves da AC-Raiz Brasileira foi utilizado o módulo de segurança criptográfico (MSC) desenvolvido pela Rede Nacional de Ensino e Pesquisa (RNP) nomeado de ASI-HSM, fornecido através de uma parceria entre as duas instituições.

Posteriormente, o software Ywyra foi concebido a partir do Ywapa e tinha como propósito criar ACs de primeiro nível e gerenciar o ciclo de vida para ACs de segundo nível. Tanto o Ywapa quanto o Ywyra foram desenvolvidos pelo Laboratório de Segurança em Computação (LabSEC) da

[1] http://www.iti.gov.br/noticias/iti-na-midia/1186-nova-identidade-civil-ajudara-a-difundir-certificado-digital-diz-iti

[2] http://rtupinamba.blogspot.com.br/2013/11/acompanhe-emissao-de-certificados-icp.html

[3] http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm

[4] Entidade autônoma

[5] http://www.iti.gov.br/programas/programa-joao-de-barro

Universidade Federal de Santa Catarina (UFSC).

A partir da demanda de certificação digital existente e que será gerada a partir do Registro de Identidade Civil (RIC), se fez necessário um sistema que possibilite a emissão de certificados para usuários finais, função não realizada pelo Ywapa nem pelo Ywyra pois são sistemas que tem como objetivo emitir certificados para outras Autoridades Certificadoras. Dessa forma, surgiu um novo componente de software chamado Hawa, que foi derivado do Ywapa e do Ywyra. Esse componente é responsável por realizar a tarefa de gerenciar o ciclo de vida do certificado digital de usuário final.

O autor deste trabalho é membro do Laboratório de Segurança em Computação (LabSEC) e contribuiu para o desenvolvimento do sistema de administração do Hawa. Pretende-se discorrer neste trabalho como esse sistema foi produzido.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Desenvolver o sistema de administração do Hawa - Sistema Gerenciador de Certificados Digitais Online.

1.1.2 Objetivos Específicos

Implementar as seguintes funcionalidades do Sistema Administrador de Autoridade Certificadora:

- Gerenciamento dos servidores;
- Gerenciamento dos vínculos de confiança;
- Configuração do número mínimo de aprovações que um certificado deve obter para ter sua emissão aprovada.

Implementar as seguintes funcionalidades do Sistema Administrador de Autoridade Registradora:

- Gerenciamento dos servidores;
- Gerenciamento dos vínculos de confiança;
- Gerenciamento dos agentes de registro;

- Gerenciamento de instalações técnicas.

1.2 MOTIVAÇÃO

O Laboratório de Segurança em Computação (LabSEC), da Universidade Federal de Santa Catarina (UFSC), tem como objetivo desenvolver projetos na área de segurança da computação, mais precisamente na área de Infraestrutura de Chaves Públicas (ICP).

O LabSEC trabalha com a missão de formar e capacitar alunos nessas áreas. O autor deste trabalho é membro efetivo do LabSEC desde o segundo semestre de 2010 e já participou de diversos projetos no âmbito de ICP, dentre eles está o Programa João de Barro, onde foram desenvolvidos os Sistemas Gerenciadores de Certificados Digitais denominados Ywapa e Ywyra.

Durante o desenvolvimento desses projetos, o autor desempenhou funções de desenvolvimento e testes do sistema e utilizou sua experiência na área da segurança da computação para a concepção desse trabalho.

1.3 JUSTIFICATIVA

A falta de um Sistema Gerenciador de Certificados Digitais que gerencie o ciclo de vida de certificados digitais para usuário final, foi uma das maiores motivações para o desenvolvimento do Hawa. Esse sistema poderá ser utilizado em conjunto com os sistemas Ywapa e Ywyra, formando assim uma hierarquia completa de uma Infraestrutura de Chaves Públicas (ICP) que passa desde a Autoridade Certificadora (AC) Raiz, pelas ACs Intermediárias até a AC Final.

Este trabalho visa então desenvolver um sistema, de solução nacional, para suprir as necessidades de um Sistema Gerenciador de Certificados Digitais Online (SGCO).

O autor elaborou esse trabalho a partir dos conhecimentos adquiridos através da participação no Programa João de Barro, além da participação nos diversos projetos ao longo de sua formação.

1.4 METODOLOGIA

As etapas para a realização do trabalho compõem de modo geral: analisar os requisitos para um Sistema de Gerenciamento de Certificados Digitais Online, observando quais suas necessidades e restrições; verificar quais

as partes do Ywapa e do Ywyra serão reaproveitadas; projetar e implementar os requisitos específicos para o Hawa provenientes do resultado da análise do projeto, produzindo um protótipo usável e partir de então realizar testes no sistema emitindo certificados digitais para usuário final.

1.5 ORGANIZAÇÃO DO DOCUMENTO

- O **Capítulo 2** mostra uma revisão bibliográfica sobre Infraestrutura de Chaves Públicas para que o leitor entenda o propósito da solução implementada e compreenda os conceitos de ICP além de informações sobre o que é um SGCO e suas principais utilidades;
- O **Capítulo 3** introduz a história do Ywapa e do Ywyra, suas funcionalidades e a motivação de eles terem sido utilizados como base para desenvolver o SGCO proposto;
- O **Capítulo 4** discorre sobre as implementações para a elaboração do sistema de administração do Hawa.
- O **Capítulo 5** por fim, apresenta as considerações finais e trabalhos futuros.

2 INFRAESTRUTURA DE CHAVES PÚBLICAS

2.1 CRIPTOGRAFIA

”A palavra criptografia significa secreto ou escrita secreta”(HOUSLEY; POLK, 2001) e é vista geralmente como embaralhamento e desenbaralhamento de mensagens. Esse mecanismo é usado quando uma pessoa precisa manter informações escondidas de quem não tem permissão para acessá-las. A criptografia pode ser utilizada, no âmbito de Infraestrutura de Chaves Públicas, para se atingir três principais objetivos(ADAMS; LLOYD, 2003), são eles: a *confidencialidade*, advinda do próprio embaralhamento da mensagem comutada entre as partes; a *integridade* que, através de modernas técnicas de criptografia, garante que qualquer alteração indevida na mensagem seja identificada; e por último temos a *autenticação*, que identifica o remetente da mensagem.

Um algoritmo criptográfico descreve uma sequência de passos que embaralha uma mensagem qualquer. Geralmente, duas entradas são necessárias para esse algoritmo, uma contendo os dados a serem embaralhados e outra contendo um valor secreto, conhecido como *chave*. Esses algoritmos são divididos em simétricos e assimétricos. Um algoritmo criptográfico simétrico usa a mesma chave para cifrar e decifrar os dados. E no algoritmo assimétrico a chave utilizada para cifrar uma mensagem é diferente da chave usada para decifrá-la. Normalmente, essas chaves são criadas em pares, ou seja, uma chave do par cifra, e a outra chave do par decifra.

2.1.1 Assinatura Digital

Uma das aplicações da criptografia assimétrica é a assinatura digital, utilizada para autenticar a fonte de uma mensagem. Essa propriedade é alcançada através do seguinte procedimento ilustrado nas figuras 1 e 2 (PIPER; MURPHY, 2002). Devemos cifrar a mensagem com uma chave privada e validar com a sua respectiva chave pública. Em termos mais práticos, como a mensagem, a qual será gerada uma assinatura, pode ser relativamente grande, é usado uma função que a partir da mensagem obtém-se um resumo único de tamanho pequeno, que é então cifrado pela chave privada para se obter a assinatura digital. Na fase da validação é feito um processo semelhante. Obtém-se um resumo da mensagem que é comparada com a assinatura decifrada pela chave pública. Se forem iguais, então a assinatura é válida.

Em (ADAMS; LLOYD, 2003), a assinatura digital é descrita da seguinte maneira:

Assinatura:

- "O assinante gera o resumo da mensagem em um valor de tamanho fixo."
- "O assinante sujeita esse valor a uma operação com a chave privada."

Verificação:

- "O verificador gera o resumo da mensagem em um valor de tamanho fixo."
- "O verificador examina esse valor, a assinatura transmitida e a chave pública da entidade que gerou a assinatura. Se a assinatura combina com a chave e com o valor do resumo, então a assinatura é verificada; caso contrário, a verificação falha."

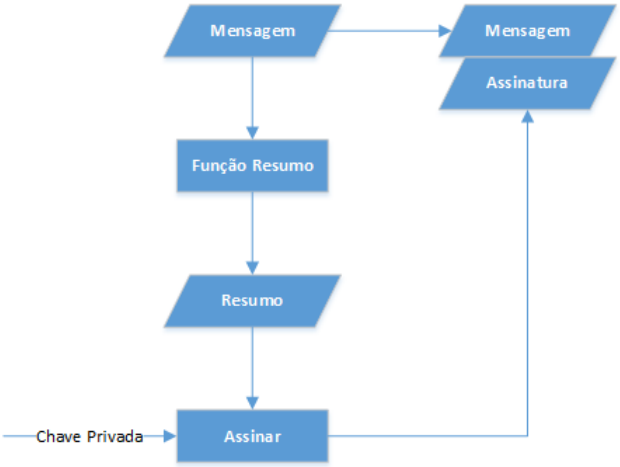

Figura 1 – Geração da Assinatura Digital.

A assinatura digital, por si só, não permite autenticar a fonte da mensagem assinada. Ela apenas permite definir qual chave foi utilizada para realizar a assinatura.

Portanto, para ser possível autenticar a fonte de uma mensagem assinada, são necessários mecanismos que permitam associar chaves com entidades, como, por exemplo, pessoas, empresas e máquinas. O certificado

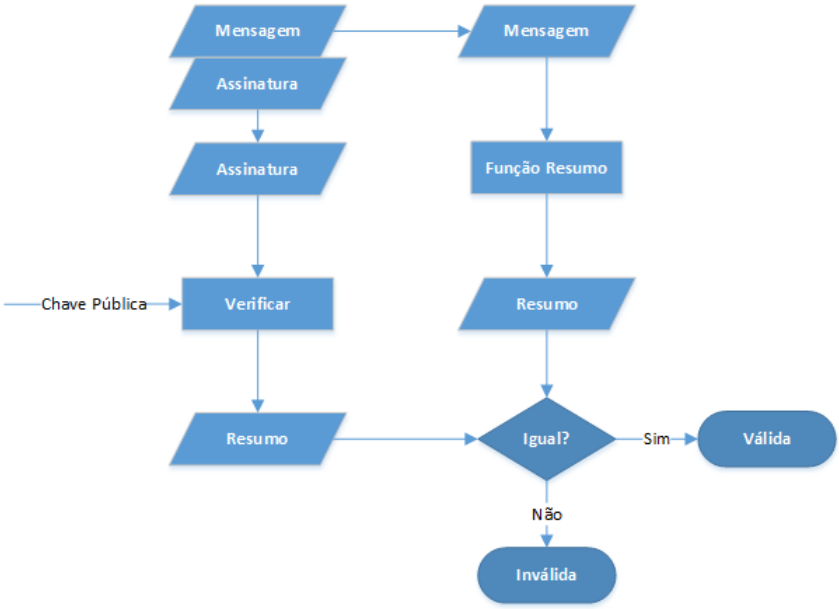

Figura 2 – Verificação da Assinatura Digital.

digital é um desses mecanismos, pois contém informações de identificação de uma entidade e sua chave pública. Na próxima seção será descrito com mais detalhes como um certificado digital funciona.

2.2 CERTIFICADO DIGITAL

O certificado tem como função, relacionar uma entidade à uma chave privada. Sempre que a chave privada for utilizada, para assinar um documento por exemplo, é possível, através do certificado, verificar a autenticidade da entidade que realizou a operação.

De acordo com (HOUSLEY; POLK, 2001), o certificado ideal deve conter nove propriedades:

- "Deve ser puramente digital, dessa forma ele pode ser distribuído pela Internet e processado automaticamente."
- "Precisa conter o nome do usuário que detém a chave privada e também informações de contato."

- “Necessita ser fácil de determinar se o certificado foi emitido recentemente.”
- “Tem que ser criado por uma terceira parte confiável ao invés do usuário que possui a chave privada.”
- “A terceira parte confiável que emitiu o certificado do usuário deve, com facilidade, identificar o certificado dele entre outros certificados emitidos.”
- “Deve ser fácil determinar se o certificado é válido ou não.”
- “O certificado deve ser inviolável.”
- “Devemos poder imediatamente determinar se a informação que está no certificado está atualizada ou não.”
- “Demanda que seja possível determinar, a partir do certificado, quais situações em que ele se aplica.”

Infelizmente, não é possível concretizar o certificado ideal. Na prática, temos diversas situações que impedem que esse artefato exista. Como credibilizar, por exemplo, a terceira parte confiável que emitiu o certificado do usuário visto que qualquer entidade pode realizar essa operação?

O certificado de chave pública define a terceira parte confiável a partir de recomendações e se apresenta portanto como o recurso que mais se assemelha ao modelo ideal.

2.3 CERTIFICADO DE CHAVE PÚBLICA

Dentre as soluções para certificado de chave pública, as duas que mais se destacam são o *Pretty Good Privacy* (PGP) e o X.509(INTERNET..., 2008). O PGP é utilizado para estruturas mais simples. Temos por exemplo a utilização do cartão de visitas digital que contém informações básicas sobre o usuário, como contato pessoal e ocupação. A proposta do PGP é que a partir da publicação do cartão via internet, outros usuários apontem se as informações são válidas ou não. Por não existir nesse modelo uma terceira parte confiável centralizada, deve-se trabalhar com confiança distribuída que fornece um nível de confiança razoável, porém pouco escalável e com problemas.

Usaremos para a realização deste trabalho o certificado baseado na especificação X.509. Ao contrário do PGP, o X.509 trabalha com a ideia de uma entidade centralizada, partindo do pressuposto que ela é inteiramente

confiável e segura. Dessa forma, podemos acreditar que as informações contidas em um determinado certificado, emitido por ela, são válidas ou não. Por outro lado, caso essa entidade seja comprometida, também teremos certeza de que todos os certificados emitidos por ela não são mais válidos.

Dentre as nove propriedades citadas anteriormente, o X.509 consegue atender as sete primeiras.

A primeira propriedade é correspondida pois o certificado é um dado digital, logo pode ser processado por um computador e facilmente distribuído pela Internet. A segunda e a terceira são realizadas pelos campos de dados que esse certificado contém, dentre eles podemos destacar, todas as informações necessárias sobre o usuário e um campo contendo a data de emissão do certificado, bem como a data de validade do mesmo. A quarta é cumprida pelo campo de emissor, o qual contém a terceira parte confiável que emitiu o certificado do usuário. Para o quinto item, temos o campo de número de série, número esse que identifica o certificado dentro do contexto da terceira parte confiável que o emitiu. As informações do emissor em conjunto com as informações que identificam o certificado, possibilitam verificar a sexta propriedade validando a assinatura digital do certificado. A sétima e última propriedade atestada pelo certificado de chave pública pode ser validada através da assinatura digital, pois se houver alguma violação no certificado, a verificação falhará.

Esse modelo se mostra uma ferramenta muito eficaz, mas não resolve a oitava nem a nona propriedade.

Para isso, novos artifícios foram criados, dentre eles a Lista de Certificados Revogados (LCR), que define quais certificados não são mais válidos, desempenhando assim a oitava propriedade e as políticas de certificação que definem que papéis um determinado certificado pode desempenhar.

2.3.1 Requisição de Certificado

Uma requisição de certificado pode ser tomada como um molde de um certificado digital, nele podemos inserir quase todas as informações necessárias para emitir um certificado, faltando apenas as informações da Autoridade Certificadora (AC) que realizará a sua emissão.

Por exemplo, se uma pessoa deseja obter um certificado digital, ela pode gerar sua requisição em casa e analisar detalhadamente se todas as informações contidas correspondem com seus dados e documentos oficiais. Dessa forma, ao chegar no local onde será realizada a emissão do certificado, a Autoridade Certificadora (AC) executa apenas uma conferência dos dados da pessoa com relação aos seus documentos, evitando possíveis erros

de digitação por funcionários da AC.

Em *Certification Request Syntax Specification*(PKCS#10..., 2000) é proposta uma sintaxe de requisição de certificado chamado *PKCS#10*. Nessa sintaxe, podemos encontrar como é definida a estrutura dessa requisição, quais campos podem ser inseridos, como informações básicas além de uma série de itens relacionados a segurança e anotações.

2.3.2 Lista de Certificados Regovados

Um certificado pode estar dentro do seu prazo de validade e não ser mais válido. Isso acontece quando uma pessoa tem sua chave privada extraviada, por exemplo. Assim, apenas com as informações contidas no certificado, não é possível saber se é válido ou não.

É preciso um artefato de suporte denominado Lista de Certificados Revogados (LCR). Essa lista contém todos os certificados emitidos por uma terceira parte confiável, que, mesmo dentro do prazo de validade, perderam sua validade. Para a identificação dos certificados dentro dessa lista, é usado o número de série do certificado.

A LCR é assinada pelo seu emissor, analogamente ao certificado. Contém uma data de emissão e outra de validade. É processada de forma similar ao certificado. Dessa forma, no momento em que alguém validar uma assinatura, deve ser feita uma consulta à LCR mais atual emitida pela Autoridade Certificadora para atestar a validade do certificado que realizou a assinatura digital.

2.3.3 Políticas de Certificação

As políticas de certificação nos informam quais são os propósitos de uso e quais restrições se aplicam à um certificado. Essas políticas são definidas pela AC e podem variar de acordo com o contexto.

2.4 AUTORIDADE CERTIFICADORA

A Autoridade Certificadora (AC) é o bloco base da Infraestrutura de Chaves Públicas (ICP)(HOUSLEY; POLK, 2001). A AC é composta por dispositivos, aplicativos e pessoas que a operam. De acordo com (HOUSLEY; POLK, 2001), uma AC deve cumprir quatro tarefas básicas:

- "Emitir Certificados (isto é, criá-los e assiná-los)."

- “Manter informações sobre o estado do certificado e emitir Lista de Certificados Revogados (LCR).”
- “Publicar seus certificados (não expirados) e LCRs atuais, de forma que os usuários podem obter as informações que eles precisam para implementar serviços de segurança.”
- “Manter arquivos de informação de estado dos certificados expirados ou revogados que a AC emitiu.”

“Uma Autoridade Certificadora (AC) pode emitir certificados para usuários, outras ACs, ou ambos”(HOUSLEY; POLK, 2001). Ao realizar essa operação, ela está vinculando uma entidade, que tem posse da chave privada, à chave pública que está contida no certificado. Outras informações dessa entidade também podem estar presentes no certificado, como endereço de email, dados de identificação, etc. A AC registra a sua identificação em todos os certificados e Lista de Certificados Revogados (LCRs) emitidos. Dessa forma, qualquer entidade que ao se deparar com um certificado, pode pesquisar pelo campo onde a identificação da AC está registrada, decidindo assim se acredita que as informações contidas no certificado são válidas ou não.

Quando um certificado perde sua validade, a AC deve garantir que uma LCR, recente, seja emitida contendo a identificação única de todos os certificados que não são mais válidos em conjunto com o certificado que perdeu a validade recentemente.

Outro aspecto importante que uma AC deve exercer, é manter arquivos e registros a longo prazo. Dessa forma, é possível que uma assinatura expedida por um certificado mantenha sua validade mesmo que o certificado em si já tenha expirado.

Percebe-se que uma AC deve exercer diversas responsabilidades para gerenciar o ciclo de vida de um certificado digital, portanto é uma tarefa comum delegar funções, diminuindo assim a sua carga total. Ela escolhe as funções que tem alta prioridade e delega as de menor para outras entidades, como por exemplo a Autoridade Registradora, a qual será descrita na próxima seção.

As ACs podem ser divididas em três categorias:

2.4.1 Autoridade Certificadora Raiz

A AC Raiz tem o seu certificado auto-assinado, ou seja, quem assina o certificado da AC é ela mesma. Na Infraestrutura de Chaves Públicas (ICP) hierárquica, ela compõe o topo da cadeia. Geralmente, ela emite certificados para ACs Intermediárias/Normativas.

2.4.2 Autoridade Certificadora Intermediária/Normativa

A AC Intermediária/Normativa tem o seu certificado emitido por uma Autoridade Certificadora Raiz ou por uma outra AC Intermediária/Normativa que tenha permissão para cumprir essa função. É essa a autoridade que emite certificados para as ACs Finais.

2.4.3 Autoridade Certificadora Final

Essa AC é responsável por emitir certificados para os usuários finais, ela está situada na parte mais inferior da cadeia hierárquica da Infraestrutura de Chaves Públicas (ICP).

A maioria dessas entidades trabalham com uma estrutura online, recebendo requisições de emissões de certificado através das Autoridades Registradoras vinculadas.

2.5 AUTORIDADE REGISTRADORA

Essa entidade não tem como função emitir certificados. Ela presta um serviço para a Autoridade Certificadora (AC), realizando todo o processo burocrático na emissão de um certificado digital.

Por exemplo, na emissão de um certificado para usuário final, o papel da Autoridade Registradora (AR) é conferir a veracidade das informações do usuário. Em outras palavras, a AR confirma para a AC se ela deve ou não emitir o certificado para o requerente.

Housley e Polk(HOUSLEY; POLK, 2001) definem dois modelos para um usuário requisitar um certificado. O primeiro é comparecer em um local físico credenciado pela AR, portando documentos de identificação pessoal, para preencher formulários e ter sua requisição de certificado gerada em conjunto com o par de chaves. O segundo modelo é usado quando o usuário não tem como se identificar previamente e já está em posse de uma requisição de certificado e de um par de chaves, enviando diretamente para Autoridade Certificadora (AC) que pode verificar que o usuário possui a chave privada correspondente à chave pública contida na requisição, mas não pode confirmar a validade dos dados. A AC deve então enviar a requisição para a AR vinculada que analisa a genuinidade dos dados e então aprova ou não a emissão do certificado.

2.5.1 Módulo Público

Esse módulo é reponsável por fazer a ponte entre o usuário final e a Autoridade Registradora. Nele, o usuário terá acesso a funções como: requisitar a emissão de certificado; pedir revogação de certificado e importar um certificado emitido. Todas esses pedidos são enviados à AR, onde são feitas as validações necessárias.

2.5.2 Módulo Agente de Registro

Esse módulo é usado pelos Agentes de Registro (AGR). Os AGRs são responsáveis por verificar os pedidos de emissão de certificado e de revogação de certificado. Na verificação eles podem, aprovar e rejeitar pedidos. Para aprovar um pedido, deve haver um número mínimo de aprovações, por parte dos AGRs, definido pela Autoridade Registradora (AR) em conjunto com a Autoridade Certificadora (AC) que ela opera.

2.5.3 Instalação Técnica

Diferentes Agentes de Registro (AGRs) podem estar cadastrados em diferentes lugares e algums podem trabalhar em um mesmo local. Para tanto foi criado o termo Instalação Técnica (IT) que representa o lugar em que AGRs operam, seja ele físico ou virtual. Os AGRs só tem permissão para operar dentro do ambiente de uma Instalação Técnica (IT). Caso ele não seja vinculado a determinada IT, não terá permissão para exercer sua funçao nesse ambiente.

2.5.4 Vínculo de Confiança

Para existir a colaboração entre uma Autoridade Certificadora (AC) e uma Autoridade Registradora (AR), é necessário um meio para interligá-las. O vínculo de confiança foi criado para atender essa demanda. Comumente esse conceito é implementado a partir da troca de certificados entre uma AC e uma AR, onde cada uma importa o certificado da outra e partilhando também informações de como elas podem acessar os seus serviços. Portanto, os vínculos de confiança são de extrema importância para funcionamento das ACs e ARs.

2.6 INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

Órgão regulamentador da certifição digital no Brasil, tem papel importante no desenvolvimento da Infraestrutura nacional. Publica regularmente documentos que descrevem como deve-se praticar a certificação digital e como devem ser implementados os sistemas que fazem uso dessa tecnologia. Uma boa parte dos documentos pode ser encontrado pela internet e estão disponíveis para qualquer usuário[1] .

[1] http://www.iti.gov.br/noticias/143-icp-brasil/legislacao/790-doc-icp

3 SISTEMA GERENCIADOR DE CERTIFICADOS DIGITAIS OFFLINE

3.1 VISÃO GERAL

O Ywapa e o Ywyra são sistemas cuja função principal é gerenciar o ciclo de vida de certificados pertencentes à uma Autoridade Certificadora (AC). O Ywapa trabalha com ACs Raízes, ou seja, os certificados de ACs gerados são auto-assinados. Por outro lado, o Ywyra trabalha com ACs Intermediárias, dessa forma as ACs geradas são constituídas por certificados emitidos por outra AC em operação.

Esse projeto surgiu da necessidade de uma solução nacional de Infraestrutura de Chaves Públicas (ICP). Foi concedido então o financiamento por parte do governo para o projeto intitulado João de Barro. Este projeto é composto por dois subprojetos: o Sistema Gerenciador de Certificados (SGC), denominado Ywapa e Ywyra, e o Módulo de Segurança Criptográfico (MSC), usado pelo SGC. O projeto teve início no ano de 2003 e foi especificado pelo Centro de Análises de Sistemas Navais - Marinha Brasileira (CASNAV)[1] .

O SGC foi desenvolvido na linguagem C++ utilizando a biblioteca Qt (QT..., 2013) para desempenhar as funções de interface gráfica. Para suprir as necessidades de criptografia, a biblioteca de código aberto OpenSSL (OPENSSL..., 2013) foi utilizada. Essa biblioteca implementa a maioria das funções criptográficas existentes atualmente e é mantida por um pequeno grupo de colaboradores. Por ser uma biblioteca de baixo nível de programação, escrita na linguagem C, o LabSEC desenvolveu um módulo, chamado LibCryptoSEC[2] , em C++ que encapsula o OpenSSL e o deixa mais abstrato, tornando o desenvolvimento mais produtivo.

Nesses sistemas podemos encontrar diversas funcionalidades pertencentes a um Sistema Gerenciador de Certificados (SGC), como por exemplo emissão de certificados, revogação de certificados, emissão de Lista de Certificados Revogados (LCR), entre outras.

3.2 FUNCIONALIDADES

As funções descritas a seguir estão divididas em três categorias:

1. Gerais: Disponíveis em todo o escopo do sistema.

[1] https://www.casnav.mar.mil.br

[2] https://projetos.labsec.ufsc.br/libcryptosec

2. Modo de Administração: Disponíveis apenas no perfil de administração.
3. Modo de Operação: Disponíveis apenas no perfil de operação.

3.2.1 Gerais

Registro de Eventos:
Todos os eventos importantes que acontecem no sistema, são registrados por meio de um *Log* onde podemos encontrar dados como data e hora da ocorrência, tipo do evento, ação executada e informações adicionais. Esses registros são de extrema importância para a auditoria do sistema.

Autenticação via Segredo Compartilhado:
A autenticação exigida pelo sistema é feita através de um grupo. Esse grupo pode ser composto por mais de um integrante. Dessa forma, é usado a autentição via segredo compartilhado, onde um segredo é quebrado em diversas partes e requer um número mínimo de membros, definido na criação do grupo, para remontá-lo. Um grupo com três membros necessita se autenticar perante o sistema e apenas dois estão presentes, mas o número mínimo de membros para se autenticar é dois. Logo, é possível remontar o segredo e realizar a autenticação.

Backup:
O *backup* do sistema existe para evitar eventuais perda de dados. Para isso, um arquivo contendo todo o conteúdo das bases de dados do sistema são cifrados e assinados para garantir a sua integridade. Para recuperar o *backup* exige-se a autenticação do perfil de administração. É possível ainda recuperar esse backup em uma versão mais recente do sistema.

Atualização Automática de Esquema da Base de Dados:
Quando uma alteração da base de dados (BD) se faz necessária, o sistema executa a atualização automática do esquema. Para isso, o sistema faz uso de uma variável que armazena a versão que o banco de dados está no momento, possibilitando assim identificar quais alterações devem ser aplicadas ao esquema do banco de dados de acordo com versão a ser atualizada.

3.2.2 Modo de Administração

Suporte à Módulos de Segurança Criptográfico via *Engine* OpenSSL:
Armazenar chaves privadas de forma segura é extremamente importante para aplicações do âmbito de Infraestrutura de Chaves Públicas. Uma alternativa é utilizar os Módulos de Segurança Criptográficos (MSC) para guardar essas chaves privadas. O Ywapa e o Ywyra implementam o suporte

à MSC via *Engine* OpenSSL. Dessa forma, qualquer MSC que utilize essa *Engine* será compatível com os sistemas.

Gerência de Autoridades Certificadoras:

No modo de administração as principais funcionalidades correspondem a criação e exclusão de Autoridade Certificadoras. No entanto, existe uma diferença entre os sistemas. No Ywapa, ao final da criação da AC, obtemos um certificado que é auto assinado; já no Ywyra, recebemos uma requisição de certificado que necessita ser enviada à uma AC em operação, para que possa realizar a emissão do certificado e posteriormente ser importado no sistema.

3.2.3 Modo de Operação

Emitir Certificado: A partir de uma requisição de certificado válida, o sistema permite emitir um certificado de forma que fará parte da hierarquia pertencente à AC.

Revogar Certificado: Dentre uma lista de certificados emitidos, é possível escolher um certificado e torná-lo inválido através da sua revogação, com opção de informar um motivo.

Emitir Lista de Certificados Revogados: Essa função é responsável por agrupar todos os certificados revogados, através de seu número de identificação, e emitir um documento (Lista de Certificados Revogados) onde será possível realizar consultas para verificar a validade de um determinado certificado.

Suporte a Modelos de Certificados:

Ao emitir um certificado, o usuário pode escolher um modelo de certificado a ser usado na operação. Esse modelo pré carrega elementos que estarão contidos no certificado emitido. Dessa forma, é possível criar modelos que contenham dados que serão usados em todas as emissões de certificados de uma determinada AC, diminuindo o esforço repetitivo do operador.

Geração de Relatórios Gerenciais: Utilizando o registro de eventos, a geração de relatórios gerenciais produz um documento que contém todos os registros executados pelo sistema e os categoriza, através de cores, de acordo com a sua severidade. Ao exportar esse relatório, deve-se indicar o intervalo de tempo desejado.

4 HAWA - SISTEMA GERENCIADOR DE CERTIFICADOS DIGITAIS ONLINE

4.1 VISÃO GERAL

O Hawa é uma solução completa para gerenciamento de certificados digitais, para ser usada online e é composto por dois ambientes: o Ambiente de Autoridade Certificadora e o Ambiente de Autoridade Registradora. Como podemos perceber na figura 3 o Ambiente de AC é composto pelos seguintes elementos:

- AC: Autoridade Certificadora;
- SAAC: Sistema Administrador de Autoridade Certificadora;
- LDAP: Servidor onde serão armazenados os certificados e as listas de certificados revogados emitidos pela AC;
- BD-AC: Base de dados da Autoridade Certificadora;
- HSM-AC: Módulo de segurança criptográfico utilizado para armazenar o par de chaves da Autoridade Certificadora.

E O Ambiente da AR é composto por:

- AR: Autoridade Registradora;
- SAAR: Sistema Administrador de Autoridade Registradora;
- BD-AR: Base de dados da Autoridade Registradora;
- HSM-AR: Módulo de segurança criptográfico utilizado para armazenar o par de chaves da Autoridade Registradora;
- Módulo Público: Sistema responsável por receber pedidos de certificados por usuários finais.

Esses elementos trabalham em conjunto para realizar a tarefa de gerenciar o ciclo de vida de certificados digitais usado por usuários finais, que podem ser: pessoas físicas, pessoas jurídicas ou equipamentos. Como se trata de uma solução nacional, o desenvolvimento do sistema tomou como base as resoluções publicadas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

De forma simples, o fluxo básico de execução do sistema em conjunto com as configurações iniciais, simulando o ciclo de vida de um certificado digital, é:

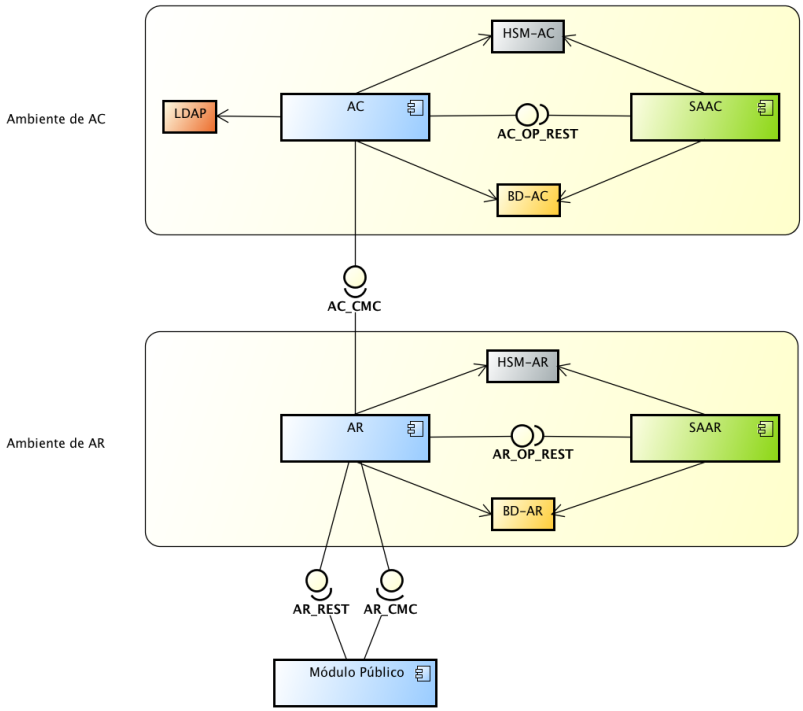

Figura 3 – Estrutura do Hawa.

1. Configurar o sistema e criar a AC e a AR através do SAAC e SAAR respectivamente.

2. Colocar a AC e a AR em operação através do SAAC e SAAR respectivamente.

3. Esperar um pedido de certificado através do Módulo Público.

4. Processar o pedido na AR, obtendo aprovação ou não dos Agentes de Registro.

5. Caso o pedido seja aprovado, enviar para AC onde será feito a emissão do certificado.

6. Publicar o certificado, através da AC, no servidor de arquivos.

7. Solicitar, através do Módulo Público, o certificado emitido.

A comunicação entre as partes é feita através de serviços *Web*, utilizando o protocolo HTTP (*HyperText Transfer Protocol*) ou HTTPS (*HyperText Transfer Protocol Secure*) dependendo da ocasião, e para o envio das requisições de certificado e certificados digitais é usado o protocolo CMC(CERTIFICATI 2008), cuja função principal é definir como essas requisições e certificados são encapsulados ao serem transmitidos pela rede.

O tipo de comunicação entre os elementos podem ser do tipo "POST" e "GET", onde a primeira submete dados a serem processados por um entidade específica e a segunda apenas requisita dados também de uma entidade específica. Ambos podem ser implementados nos protocolos citados anteriormente, o HTTP e o HTTPS, onde a diferença está em que o primeiro transmite os dados em texto plano e o segundo em texto cifrado.

Devido a similaridade das suas funções, o Hawa pôde ser desenvolvido com base no código do Ywapa e do Ywyra, visto que muitas funções puderam ser diretamente reutilizadas e outras reaproveitadas através de pequenas modificações em suas implementações. Dessa forma, o código do projeto foi ramificado e as alterações foram efetuadas.

O projeto desenvolvido neste trabalho apresenta a implementação dos dois Sistemas de Administração, destacados pela cor verde na figura 3. São eles:

- SAAC: Sistema Administrador de Autoridade Certificadora
- SAAR: Sistema Administrador de Autoridade Registradora

4.2 DIFERENÇAS E FUNÇÕES REUTILIZADAS

Diferente do Ywapa e do Ywyra, os sistemas de administração do Hawa (SAAC e SAAR) não são responsáveis por realizar emissão de certificados digitais, revogação de certificados digitais e emissão de LCRs. As funções atribuídas aos sistemas de administração correspondem à:

SAAC:

- criar autoridade certificadora;
- gerenciar o servidor da AC (iniciar, parar, verificar estado e configurar);
- gerenciar vínculos de confiança com autoridades registradoras;
- definir o número mínimo de aprovações que um pedido de certificado deve obter antes de ser aprovado

SAAR:

- criar autoridade registradora;
- gerenciar o servidor da AR (iniciar, parar, verificar estado e configurar);
- gerenciar vínculos de confiança com autoridades certificadoras;
- gerenciar instalações técnicas;
- gerenciar agentes de registro

As principais funcionalidades reutilizadas do Ywapa e do Ywyra, descritas na seção 3.2, foram:

1. autenticação via segredo compartilhado;
2. backup;
3. atualização automática de esquema de base de dados;
4. suporte à MSC via Engine OpenSSL;
5. gerência de autoridades certificadoras e autoridades registradoras;
6. geração de relatórios gerenciais

4.3 PROCESSO DE DESENVOLVIMENTO

Durante o desenvolvimento do projeto, diversas pessoas trabalharam em conjunto para que a solução do Hawa fosse concluída. Para organizar e gerenciar esse grupo, diversas diretrizes foram adotadas para alcançar o sucesso.

Os gerentes de projeto utilizavam uma plataforma online, chamada de *Trac*[1] onde foram criadas tarefas, denominadas de *ticket*, relacionadas com a implementação do projeto e as repassavam aos desenvolvedores. A partir disso, os desenvolvedores executavam a tarefa e a documentavam na plataforma *Trac*. Depois disso, repassavam o *ticket* para o gerente de qualidade. Esse gerente era responsável por analisar a solução proposta pelo desenvolvedor e fornecer uma resposta autorizando ou não a solução. Caso ela fosse aceita, a tarefa era encerrada e dada como realizada com sucesso, caso contrário, retornaria ao desenvolvedor que deveria melhorar sua solução até que fosse aceita.

[1] http://trac.edgewall.org/

As tarefas que a equipe executou originavam de duas principais fontes. Uma delas era a própria equipe, que de acordo com os problemas que surgiam ao decorrer do projeto, criavam tarefas para resolvê-los. Outra fonte era o Instituto Nacional de Tecnologia e Informação[2] (ITI). O ITI foi o orgão financiador do projeto e portanto estava conectado diretamente com o desenvolvimento de requisitos do projeto. Na figura 4(WERLANG; MARTINS, 2010) está descrito em detalhes esse processo.

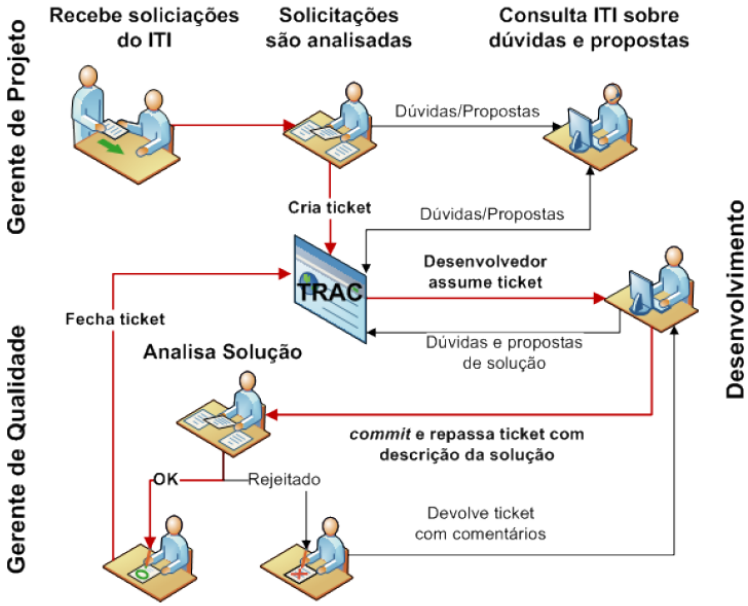

Figura 4 – Processo de Desenvolvimento.

4.4 FUNCIONALIDADES IMPLEMENTADAS

Nessa seção serão apresentadas as funções implementadas pelo autor do projeto, serão descritos os detalhes de cada item e ao final de cada subseção são apresentados os artefatos gerados. Os requisitos identificados desenvolvidos nessa seção foram provenientes dos documentos especificados pela ICP-Brasil denominados Manual de Condutas Técnicas 11 - Volume I:

[2] http://www.iti.gov.br/

Requisitos, Materiais e Documentos Técnicos para Homologação de Software de Autoridade Certificadora (AC) e Autoridade de Registro (AR) no Âmbito da ICP-Brasil[1] e Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades de Certificação da ICP-Brasil[2] (DOC-ICP-05).

4.4.1 Gerenciamento de Servidores

A fim de gerenciar os servidores, foram implementadas as funções para que fosse possível configurar e iniciar os servidores através do sistema de administração. Essas funções enviam requisições para serviços hospedados na internet, através da tecnologia de *web service*, disponibilizados pelos servidores do Hawa.

A seguir, encontra-se a descrição da lista das funções implementadas para o gerenciamento dos servidores:

- **Configurar:** função responsável por configurar os dados de acesso ao servidor, tais como o endereço *Web* do serviço disponibilizado pelo módulo *Online*.
- **Iniciar:** envia uma requisição HTTP "POST" ou HTTPS "POST" com as seguintes informações: A identificação do banco de dados a ser utilizado em conjunto com a porta que o sistema está escutando, o endereço de acesso à máquina que está hospedando o banco de dados, a senha e o usuário para acessar o base de dados e a chave simétrica do perfil de operação do módulo de admistração, a qual será usada para decifrar os dados.
- **Parar:** envia uma requisição HTTP "POST" ou HTTPS "POST" para o endereço do serviço cuja função é cessar o serviço do servidor. Um exemplo de execução dessa função com a intenção de parar o servidor de uma determinada Autoridade é: Mandar uma requisição para o endereço "http://meuservidor.com/hawa-ca/idDaAutoridade/stop" onde o parâmetro "hawa-ca" indica qual módulo está sendo executado, o "idDaAutoridade" informa a identificação da Autoridade que está sendo requisitada para suspender o servidor e "stop" indica a ação de parar.
- **Verificar Estado:** envia uma requisição HTTP "GET" ou HTTPS "GET" e recebe como resposta os seguintes textos: "OPERATING" ou "UNA-

[1] http://www.iti.gov.br/images/servicos/homologacao/MCT_11_1.pdf

[2] http://www.iti.gov.br/images/icp-brasil/Normas%20ICP-Brasil/Documentos%20principais/DOC_ICP_05_Requisitos_Minimos_para_Declaracoes_de_Praticas_de_Certificacao_das_AC.pdf

VAILABLE" ou seja, que o servidor está operando ou parado respectivamente.

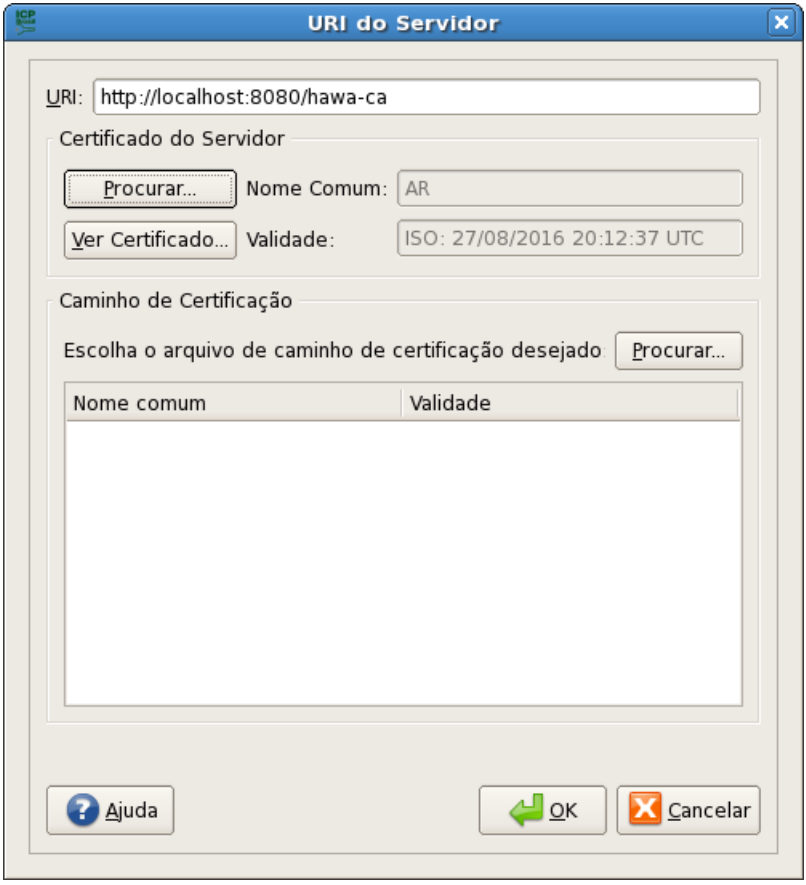

Figura 5 – Configuração do Servidor da Autoridade Registradora.

Essas requisições, por questões de segurança, são enviadas pelo protocolo HTTPS citado na seção 4.1, o qual tem como função principal cifrar os dados a serem enviados pela internet. Dessa forma, dificulta-se ataques externos.

Os seguintes artefatos foram criados a partir da implementação do gerenciamento de servidores:

- Classe *Server*: representa a abstração de um servidor real, armazenando todas as informações necessárias que o servidor precisa para executar suas funções.
- Classe *ServerThread*: responsável por enviar as requisições HTTP ao servidor.
- Classe *ServerController*: responsável por montar as requisições HTTP a partir de informações obtidas por objetos da classe "Server". Repassa essas requisições para a classe "ServerThread", para então ser enviada ao seu destino.
- Classe *ServerStorageManager*: responsável por realizar as funções de persistência de objetos da classe "Server".
- Classe *ServerURL*: interface gráfica responsável por receber os dados de entradas do usuário na configuração do servidor.

4.4.2 Gerenciamento dos Vínculos de Confiança

Como visto na seção 2.5.4 percebe-se que os vínculos de confiança são muito importantes para uma Autoridade Certificadora. Eles informam quais são as Autoridades Registradoras que estão vínculadas e, dessa forma, autorizadas a enviar requisições para a tal AC. O mesmo se aplica no contexto da AR. Para uma AR poder exercer sua função, ela obrigatoriamente necessita estar vinculada a uma AC.

A seguir está descrita a lista das funções implementadas para o gerenciamento dos vínculos de confiança entre AC e AR:

- **Registrar:** registra um novo vínculo de confiança. Informações necessárias para concluir a operação:
  - **Sistema de Administração de Autoridade Certificadora:** nome do vínculo, endereço *Web* onde está localizado o servidor da AR e o certificado da Autoridade Registradora.
  - **Sistema de Administração de Autoridade Registradora:** nome do vínculo, endereço *Web* onde está localizado o servidor da AC, diretório *Lightweight Directory Access Protocol* (LDAP) onde serão publicados os certificados e as LCRs emitidos pela AC vinculada e o certificado da Autoridade Certificadora.
- **Configurar:** nessa opção é possível alterar alguma informação de um vínculo pré-registrado.

- **Habilitar ou Desabilitar:** responsável por tornar um vínculo habilitado ou desabilitado. Caso o vínculo fique desabilitado, a AC não aceitará requisições da AR vinculada.

- **Remover:** remove um vínculo a partir da lista de vínculos existentes.

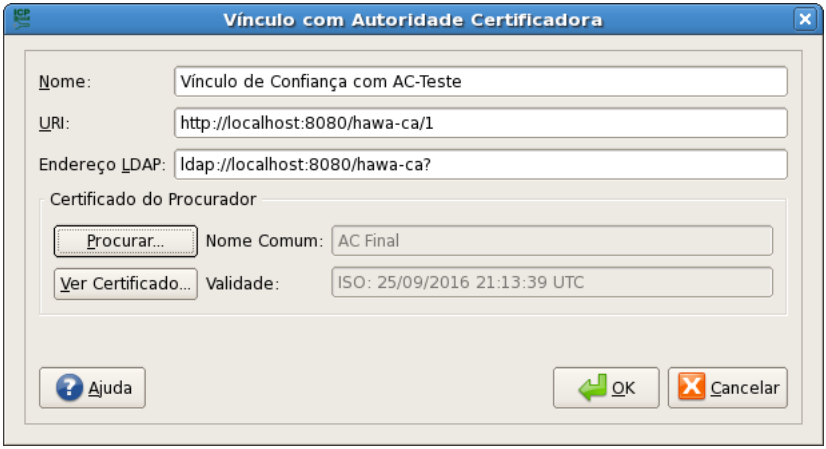

Figura 6 – Registro do Vínculo de Confiança com Autoridade Certificadora.

Os seguintes artefatos foram criados a partir da implementação do gerenciamento dos vínculos de confiança:

- Classe *TrustedAuthoritySettings*: abstrai uma entidade do vínculo de confiança. Guarda as informações de um determinado vínculo.

- Classe *TrustedAuthorityStorageManager*: responsável por realizar as funções de persistência de objetos da classe *TrustedAuthoritySettings*.

- Classe *TrustedAuthority*: interface gráfica responsável por receber os dados de entradas do usuário no registro do vínculo de confiança.

- Classe *TrustedAuthorityManager*: interface gráfica responsável por gerenciar os vínculos de confiança. Nessa janela estão disponíveis todas as funções citadas anteriormente.

4.4.3 Gerenciamento das Instalações Técnicas

Funcionalidade presente apenas no módulo de administração da Autoridade Registradora, tem como objetivo gerenciar Instalações Técnicas (IT). As quais servem para serem vinculadas aos Agentes de Registro (AGR). Dessa forma, AGRs só podem operar em uma determinada IT caso estejam associados à ela. As funções implementadas foram:

- **Registrar:** registra uma nova IT. Informação necessária para completar a operação: Nome da IT.
- **Configurar:** nessa opção é possível configurar uma IT previamente registrada.
- **Habilitar ou Desabilitar:** responsável por tornar uma IT habilitada ou desabilitada. Caso a IT fique desabilitada, a AR não permitirá que os AGRs a acessem.
- **Remover:** remove uma IT a partir da lista de ITs existentes.

Artefatos produzidos:

- Classe *TechnicalInstallation*: abstrai uma entidade da instalação técnica. Guarda informações como: Nome da IT e estado da IT, que nos informa se ela está habilitada ou não.
- Classe *TechnicalInstallationStorageManager*: responsável por realizar as funções de persistência de objetos da classe *TechnicalInstallation*. Funções principais: Recuperar, salvar, atualizar e mudar estado.
- Classe *TechnicalInstallationBase*: interface gráfica responsável por receber os dados de entradas do usuário no registro da IT.
- Classe *TechnicalInstallationManager*: interface gráfica responsável por gerenciar as ITs. Nessa janela estão disponíveis todas as funções citadas anteriormente.

4.4.4 Gerenciamento dos Agentes de Registro

Funcionalidade presente apenas no módulo de administração da Autoridade Registradora, tem como objetivo gerenciar Agentes de Registro (AGR).

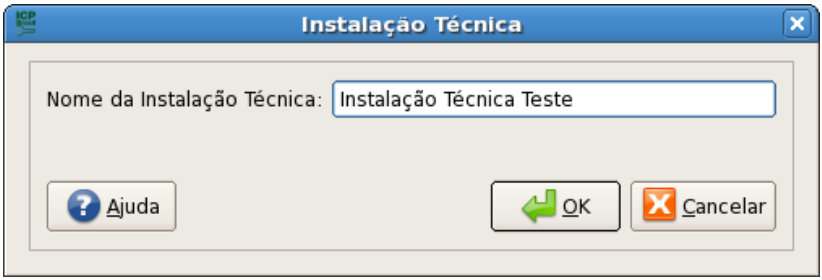

Figura 7 – Registro da Instalação Técnica.

Os AGRs são responsáveis por operar uma AR e exercem funções do tipo: Aprovar ou Rejeitar um pedido de emissão de certificado.

A seguir são apresentadas as funções implementadas para o gerenciamento dos AGRs:

- **Registrar:** função responsável por registrar um novo AGR no sistema. Para realizar essa operação, é preciso informar: Nome do AGR e certificado digital que será utilizado para assinar as suas operações na AR. Esse certificado pode ser carregado através de um arquivo ou de um cartão inteligente que armazena certificados conhecido por *smart card*. Nessa opção também é possível vincular os AGRs às instalações técnicas disponíveis.
- **Configurar:** modificar as informações dos AGRs registrados e configurar seus vínculos caso não isso não tenha sido feito na operação de registro.
- **Habilitar/Desabilitar:** responsável por tornar um AGR habilitado ou desabilitado. Caso o Agente de Registro (AGR) fique desabilitado, não será possível se autenticar com esse AGR para operar a AR.
- **Remover:** remove um AGR a partir da lista de AGRs existentes.

Artefatos produzidos:

- Classe *RegistrationAuthorityOfficer*: classe que abstrai uma entidade do Agente de Registro (AGR). Guarda informações como: Nome do AGR, certificado, estado e instalações técnicas vinculadas.
- Classe *RegistrationAuthorityOfficerStorageManager*: responsável por realizar as funções de persistência de objetos da classe *Registratio-*

nAuthorityOfficer. Funções principais: Recuperar, salvar, atualizar, salvar certificado do AGR e mudar estado.

- Classe *RegistrationAuthorityOfficerBase*: interface gráfica responsável por receber os dados de entradas do usuário no registro do AGR.
- Classe *RegistrationAuthorityOfficerManager*: interface gráfica responsável por gerenciar os AGRs. Nessa janela estão disponíveis todas as de gerência dos AGRs.

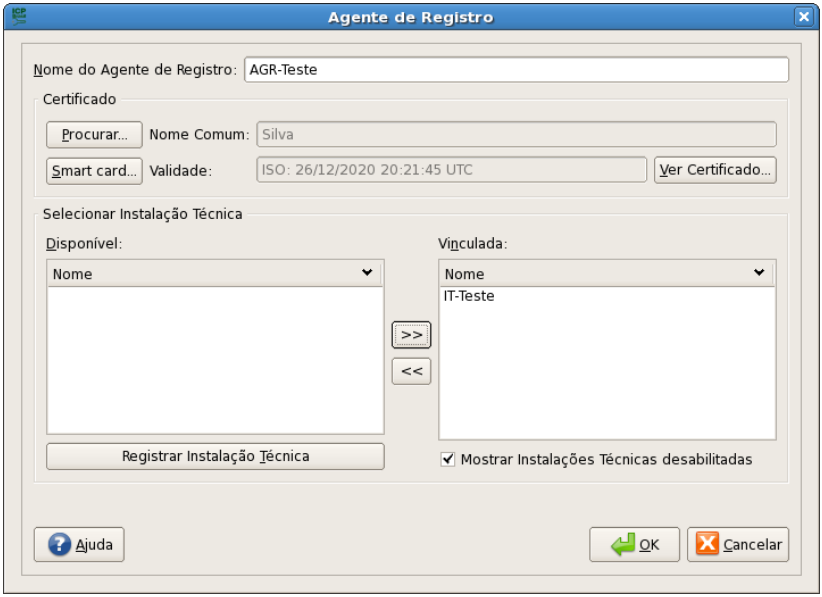

Figura 8 – Cadastro do Agente de Registro.

4.4.5 Configuração do Número Mínimo de Aprovações

Ao receber um pedido de emissão de certificado a partir de um usuário final, esse pedido entra em estado de aprovação, onde os AGRs devem aceitá-lo ou não.

Nessa subseção trataremos da função que define o número mínimo de aprovações que um pedido deve obter para que avance para o próximo estágio da emissão de certificado.

A função implementada nesse tópico é simples, porém importante para a operação da AR. Essa função está presente apenas no sistema de administração da AR.

Configurar: Modificar o valor referente ao número mínimo de aprovações que um pedido de certificado necessita obter para ter sua emissão aprovada.

Artefato gerado: Classe *RAOMinimumNumberApprovals*: interface gráfica responsável por receber os dados de entradas do usuário na configuração do número mínimo de aprovações.

As demais implementações foram realizadas dentro das classes que trabalham diretamente com a implementação da Autoridade Registradora, pois se trata de um novo atributo da AR.

4.5 ALTERAÇÕES NA BASE DE DADOS

A base de dados do Hawa foi desenvolvida a partir das que existiam para o Ywapa e o Ywyra, no entanto diversas modificações foram realizadas, a fim de satisfazer os requisitos de um sistema gerenciador de certificados digitais online. A primeira mudança foi concentrar todas as informaçoes em uma única base de dados protegida por senha e com os dados sigilosos cifrados. Anteriormente, existiam duas bases de dados, uma protegida por senha e outra não. Dessa forma, informações que não deveriam ser públicas estavam expostas para qualquer usuário com acesso ao dispositivo que mantém as bases de dados. Porém, para poder realizar acesso à base de dados, o Hawa deve saber quais são os dados de acesso. Tais dados, são mantidos em uma base de dados externa onde contém apenas as informações necessários ao acesso, mantendo esses dados cifrados.

Para a base de dados protegida utilizou-se o MySQL[1] e para a aberta o SQLite[2], ambos sistemas gratuitos e *Opensource*.

Outra funcionalidade implementada, foi a possibilidade de manter a base de dados em uma máquina remota, ou seja, é possível configurar o sistema em um ambiente e a base de dados em outro, realizando acesso através da rede. Para isso, adaptações na configuração do acesso à base de dados foram feitas, possibilitando a inserção do endereço de rede que a base de dados está hospedada como mostrado na figura 9.

A partir da alternativa de se manter a base de dados em uma máquina remota, foi necessário alterar a forma em que o sistema é inicialmente configurado. Modificou-se o configurador da base de dados para que fosse possível configurar os componentes de forma separada. A configuração herdada do

[1] http://www.mysql.com/

[2] http://www.sqlite.org/

sistema Ywapa e Ywyara portanto, corresponde ao acesso do sistema e da base de dados a partir da mesma máquina.

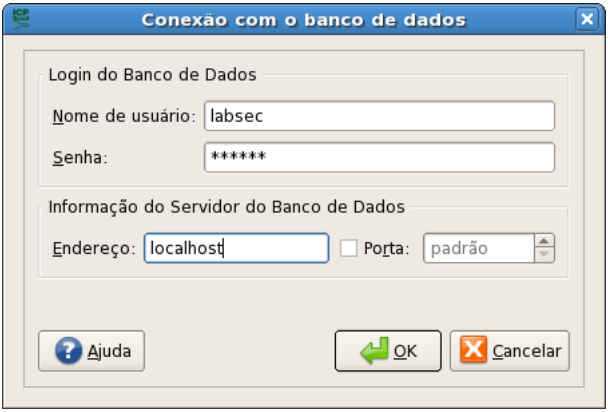

Figura 9 – Conexão com a base de dados.

5 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo apresentar a implementação de dois sistemas: Sistema Administrador de Autoridade Certificadora (SAAC) e Sistema Administrador de Autoridade Registradora (SAAR). No capítulo 3 foi demonstrado a aplicação que serviu como base para o desenvolvimento do projeto. E no capítulo 4 foram descritas as contribuições realizadas pelo autor do projeto.

Um dos objetivos do trabalho era implementar as funcionalidades do Sistema de Administrador de Autoridade Certificadora, que engloba funções como: gerenciamento de servidores, gerenciamento dos vínculos de confiança e definição do número mínimo de aprovações. Outro objetivo era desenvolver as funcionalidades para o Sistema Administrador de Autoridade Registradora (SAAR), com funções semelhantes ao objetivo anterior, porém contendo itens diferentes como: gerenciar agentes de registro e gerenciar instalações técnicas.

As melhorias na base de dados também se mostraram importantes, pois tornaram o sistema mais flexível promovendo maneiras diferentes de configurar a base de dados em relação ao sistema.

Uma das limitações do trabalho que não obteve solução foi a atualização das operações realizadas no servidor. Ao executar a operação de iniciar um servidor, por exemplo, qualquer alteração que seja realizada nas configurações do sistema, enquanto o servidor estiver operando, não são refletidas em tempo real. É necessário parar o servidor, realizar as configurações e então colocar novamente o servidor em operação.

De forma geral, a contribuição deste trabalho foi de desenvolver os sistemas de administração de um Sistema de Gerenciador de Certificados Digitais Online (SGCO) que são utilizados para configurar os parâmetros da Autoridade Certificadora (AC) e da Autoridade Registradora (AR). Esses sistemas são integrantes fundamentais da solução Hawa, que tem como função gerenciar o ciclo de vida dos certificados digitais de usuário final.

5.1 TRABALHOS FUTUROS

Apesar deste trabalho desenvolver sistemas de administração inteiramente funcionais, ainda é necessário produzir algumas funcionalidades que tem o objetivo de aprimorar os sistemas como um todo. As principais atividades observadas são:

- **Atualização Automática das Configurações:** ao configurar o ambi-

ente da AC, necessitamos iniciar o servidor de modo que os serviços da AC entrem em operação. Dessa forma, todas as configurações realizadas antes de iniciar o serviço são carregadas. Quando uma eventual mudança no contexto da AC necessita ser realizada, devemos para o serviço da Autoridade Certificadora (AR) e efetuar as alterações previstas, retomando em seguida a execução do servidor.

Deve-se alterar a forma como os dados configurados da AC são carregados. Ao entrar em operação, todas as modificações posteriores da Autoridade Certificadora (AC) devem ser carregadas em tempo real, evitando que o serviço seja interrompido. Importante ressaltar que podemos ter problemas de acesso concorrido aos dados, principalmente quando a AC está sendo requisitada constantemente.

- **Certificado Procurador:** os certificados digitais usados na criação dos vínculos de confiança, geralmente são os certificados da própria Autoridade Certificadora (AC) ou da Autoridade Registradora (AR). Isso não é bom, pois usar esses certificados para propósitos que não são os idealizados, tornam a entidade enfraquecida. Para isso, um certificado digital deve ser gerado, ao final da criação da AC ou da AR, que contenha os mesmos dados de identificação do certificado digital da AC ou da AR, porém faz uso de um par de chaves diferente.

- **Importar Configurações Externas da Autoridade Certificadora:** na etapa de configuração da AC diversas informações devem ser fornecidas. Algumas delas são adquiridas por meio de um arquivo externo ao escopo do sistema. Nesse arquivo estão contidas configurações como: Políticas de Certificação, Endereço e Senha LDAP e por último o Diretório de Publicação da Lista de Certificados Revogados. Propõe-se que essas configurações sejam importadas para o sistema, criando assim tabelas na base de dados para armazenar essas informações e interfaces de usuário para receber esses dados.

REFERÊNCIAS BIBLIOGRÁFICAS

ADAMS, C.; LLOYD, S. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. [S.l.]: Addison-Wesley, 2003. 321 p.

CERTIFICATE Management over CMS (CMC). [S.l.], Junho 2008. <http://www.ietf.org/rfc/rfc5272.txt>. Acessado em 30/10/2013.

HOUSLEY, R.; POLK, T. *Planning for PKI: Best Practices Guide For Deploying Public Key Infrastructure*. [S.l.]: Wiley, 2001. 352 p.

INTERNET X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. [S.l.], Maio 2008. <http://www.ietf.org/rfc/rfc5280.txt>. Acessado em 22/06/2012.

OPENSSL: The Open Source toolkit for SSL/TLS. [S.l.], Dezembro 2013. <http://www.openssl.org/>. Acessado em 20/10/2013.

PIPER, F.; MURPHY, S. *Cryptography: A Very Short Introduction*. [S.l.]: Oxford, 2002. 142 p.

PKCS#10: Certification Request Syntax Specification Version 1.7. [S.l.], Novembro 2000. <http://www.ietf.org/rfc/rfc2986.txt>. Acessado em 14/10/2013.

QT, The Cross-Platform Application Framework. [S.l.], 2013. <http://qt.digia.com/>. Acessado em 20/10/2013.

WERLANG, F. C.; MARTINS, L. G. *Sistema Gerenciador de Certificados Offline*. Brazil: [s.n.], 2010.