UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

ICP-UFSM: INFRA-ESTRUTURA DE CHAVES PÚBLICAS PARA A UNIVERSIDADE FEDERAL DE SANTA MARIA

TRABALHO DE GRADUAÇÃO

Diego Mostardeiro Friedrich

Santa Maria, RS, Brasil
2008

ICP-UFSM: INFRA-ESTRURA DE CHAVES PÚBLICAS PARA A UNIVERSIDADE FEDERAL DE SANTA MARIA

por

Diego Mostardeiro Friedrich

Trabalho de Graduação apresentado ao Curso de Ciência da Computação da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção do grau de
Bacharel em Ciência da Computação

Orientadora: Profª. Drª. Roseclea Duarte Medina

Trabalho de Graduação Nº 245
Santa Maria, RS, Brasil
2008

Universidade Federal de Santa Maria
Centro de Tecnologia
Curso de Ciência da Computação

A Comissão Examinadora, abaixo assinada,
aprova o Trabalho de Graduação

ICP-UFSM: INFRA-ESTRUTURA DE CHAVES PÚBLICAS PARA A UNIVERSIDADE FEDERAL DE SANTA MARIA

elaborado por
Diego Mostardeiro Friedrich

como requisito parcial para obtenção do grau de
Bacharel em Ciência da Computação

COMISSÃO EXAMINADORA:

Roseclea Duarte Medina, Drª.
(Presidente/Orientadora)

Oni Reasilvia Sichonany, Mscª. (UFSM)

Raul Ceretta Nunes, Dr. (UFSM)

Santa Maria, 1º de fevereiro de 2008.

AGRADECIMENTOS

Primeiramente, agradeço a Deus por ter me dado a oportunidade de estar no mundo.

Aos meus pais, Amália Mostardeiro Friedrich e Bruno Augusto Friedrich, agradeço todo o amor e apoio, sem eles nada disso seria possível, minhas irmãs Bruna e Luana Mostardeiro Friedrich, minha namorada Graziele Streck Lovato e ao restante da minha família.

Gostaria de agradecer também o professora Roseclea Duarte Medina, pela atenção, carinho e auxílio nas atividades e discussões sobre o andamento e dúvidas desta monografia de conclusão de curso, assim como sua amizade em todos os momentos durante a graduação.

Por fim, a todos os meus verdadeiros amigos de Florianópolis, Restinga Sêca e, inclusive, os colegas do curso, especialmente ao Eduardo Maikel Müller, Jonathan Alves, Juliano da Costa e Tiago Nonoai, que torceram por mim e estiveram presentes nesta caminhada.

RESUMO

Trabalho de Graduação
Curso de Ciência da Computação
Universidade Federal de Santa Maria

ICP-UFSM: INFRA-ESTRUTURA DE CHAVES PÚBLICAS PARA A UNIVERSIDADE FEDERAL DE SANTA MARIA

Autor: Diego Mostardeiro Friedrich
Orientadora: Profª. Drª. Roseclea Duarte Medina
Local e data da defesa: Santa Maria, 1º de fevereiro de 2008.

A partir do projeto Infra-estrutura de Chaves Públicas Educacional (ICP-EDU) que desenvolve ferramentas com o objetivo de melhorar a segurança digital no âmbito acadêmico, dando suporte ao cotidiano das universidades brasileiras, têm-se como objetivo deste trabalho, estudar e pesquisar sobre o assunto a fim de elaborar uma proposta de implementação de uma ICP para a Universidade Federal de Santa Maria (UFSM). O resultado apresentado é uma sugestão de implementação que tenta se enquadrar melhor dentro das necessidades da UFSM, tendo em vista que a mesma possa ser colocada em prática, se possível, para beneficiar a comunidade acadêmica através da utilização do software desenvolvido pelo grupo de trabalho ICP-EDU.

Palavras-chave: Infra-estrutura de Chaves Públicas; Segurança Digital; Grupo de Trabalho ICP-EDU.

ABSTRACT

Undergraduation Final Work
Undergraduation in Computer Science
Federal University of Santa Maria

PKI-UFSM: PUBLIC KEY INFRASTRUCTURE FOR THE FEDERAL UNIVERSITY OF SANTA MARIA

Author: Diego Mostardeiro Friedrich
Advisor: Roseclea Duarte Medina

From the project of Public Key Infrastructure Educational (PKI-EDU) that develops tools with the objective to improve the digital security in the academic scope, giving support to the daily activities of the Brazilian universities, this work has the target, to study and to search about the subject in order to develop a proposal for implementation of an PKI for the Federal University of Santa Maria (UFSM). The presented result is an implementation suggestion that tries to be fit better into the necessities of the UFSM, if this implementation can be put in practice, it can, benefit the academic community through the use of a software developed for the work group PKI-EDU.

Keywords: Public Key Infrastructure; Digital Security; Work Group PKI-EDU.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
AR	Autoridade de Registro
DSA	Digital Signature Algorithm
DP	Diretório Público
EAD	Educação à Distância
HSM	Hardware Secure Module
HUSM	Hospital Universitário de Santa Maria
ICP	Infra-estrutura de Chaves Públicas
ICP-Brasil	Infra-estrutura de Chaves Públicas Brasileira
ICP-EDU	Infra-estrutura de Chaves Públicas Educacional
IES	Instituição de Ensino Superior
IP	Internet Protocol
LabSEC	Laboratório de Segurança em Computação
LCR	Lista de Certificados Revogados
MD5	Message Digest Nº 5
MEC	Ministério da Educação
MP	Módulo Público
OpenSSL	Open Secure Sockets Layer
PCD	Pacote de Certificação Digital
PHP	Hypertext Preprocessor
PKI	Public Key Infrastructure
RNP	Rede Nacional de Ensino e Pesquisa
RSA	Rivest, Shamir e Adelman
SEEP	Secretaria de Educação Especial
SGCI	Sistema de Gerenciamento de Certificados ICP-EDU
SHA-1	Secure Hash Algorithm 1
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UAB	Universidade Aberta do Brasil
URL	Uniform Resource Locator
XML	eXtensible Markup Language
Web	Teia, fazendo menção à rede que se estabelece com a Internet

SUMÁRIO

INTRODUÇÃO

A insegurança está cada vez mais presente no dia-a-dia das cidades e do mundo como um todo, por isso, passamos a tomar medidas mais rígidas para que fatos desagradáveis não venham a nos comprometer. No meio digital o mesmo comportamento vem tomando mais espaço a cada dia através de pesquisas, implementações e atitudes que têm como premissa aumentar a segurança das informações compartilhadas através da Internet.

A certificação digital é um das maneiras pela qual é possível obter aumento no nível de segurança ao enviar e receber informações no meio digital. Ela atesta a identidade de uma pessoa ou instituição na Internet por meio de um arquivo eletrônico assinado digitalmente garantindo, assim, autenticidade, integridade e o não-repúdio de documentos assinados ou transações efetuadas, além da confidencialidade entre as partes.

Nessa área, a grande dedicação em pesquisa e desenvolvimento de ferramentas e o aperfeiçoamento da tecnologia é conseqüência, por exemplo, da intensidade na qual vem crescendo a alternativa da substituição do papel por documentos eletrônicos seguros e pela busca por segurança nas transações, já que o comércio eletrônico, de acordo com a e-Bit (2007), vem quebrando recordes de faturamento a cada ano que passa.

Com o propósito de dispor uma alternativa ao mercado no ramo de certificação digital que existia no País, em 2003, a Rede Nacional de Ensino e Pesquisa (RNP) lançou uma chamada pública de projetos. Estes deveriam apresentar soluções viáveis para a implantação de uma infra-estrutura capaz de dar suporte ao cotidiano das universidades brasileiras.

Essa chamada teve como vencedor o projeto Grupo de Trabalho Infra-estutura de Chaves Públicas Educacional (GT ICP-EDU), equipe que originou cooperação entre algumas Instituições de Ensino Superior (IES) do País, tais como a Universidade Federal de Minas Gerais (UFMG), a Universidade Federal de Santa Catarina (UFSC) e a Universidade Estadual de Campinas (Unicamp), com o objetivo de melhorar a segurança digital no âmbito acadêmico, o qual atualmente está em sua terceira fase, conforme a RNP (2007).

Tem-se como objetivo do presente trabalho estudar e pesquisar sobre os resultados obtidos pelo GT ICP-EDU, com o propósito de apresentar uma proposta de implementação de uma Infra-estrutura de Chaves Públicas (ICP) para a comunidade acadêmica da UFSM através da utilização do Sistema de Gerenciamento de Certificados (SGC), desenvolvido por tal grupo de trabalho.

Afinal, devido ao fato do crescimento do uso de certificação digital no Brasil e no mundo, as universidades brasileiras também vêm desenvolvendo e aderindo a essa nova tecnologia. Contudo, a UFSM encontra-se entre as instituições que ainda não usufruem e não oferecem este tipo de serviço para sua comunidade acadêmica.

Essa tecnologia poderá funcionar como grande aliada da Universidade e de seus usuários, pois o ambiente acadêmico utiliza um tráfego digital de informações importantes como históricos escolares, resultados de pesquisas, notas de provas, informações financeiras, informações médicas, etc.

Outro aspecto importante a considerar é a participação da UFSM em projetos de Educação a Distância (EAD) como a Rede Gaúcha de Ensino Superior a Distância (REGESD). Esta rede é formada por 8 (oito) instituições de ensino superior do RS, as quais oferecem, em parceria, 6 (seis) cursos de graduação e compartilham as informações acadêmicas, financeiras e administrativas destes via rede.

Já na Universidade Aberta do Brasil (UAB) a UFSM oferece os cursos de graduação e pós-graduação sem parcerias, mas as trocas de informações ocorrem com o Ministério da Educação (MEC), através da integração dos sistemas da UFSM (acadêmico, financeiro, administrativo e ambiente virtual de aprendizagem) com o mesmo, gerando também intenso tráfego de informações importantes e sigilosas.

Ainda, conforme Zen (2008), o Hospital Universitário de Santa Maria (HUSM), possui em desenvolvimento uma reimplementação de seu sistema de gerenciamento de informações dos pacientes da Unidade de Cardiologia. Contudo, parte importante deste sistema não foi devidamente focada na reimplementação. Esta parte é a área da segurança, pois atualmente a nova aplicação conta com um simples sistema de login.

Nesse contexto, as discussões para o uso de certificação digital ganharam magnitude na Instituição, porém os custos envolvidos para a adoção de uma

certificação digital privada (que é calculado por aluno matriculado) inviabilizou o processo, dando origem então a este trabalho de graduação*, que iniciou com uma pesquisa por uma solução alternativa de certificação digital.

Atualmente, existe a necessidade de implantação de um serviço de emissão de certificados digitais que forneça bons níveis de criptografia e segurança para realizar transações confiáveis e autenticação de usuários.

Através deste trabalho será, então, realizada uma análise de quais são os fatores relevantes para a implantação de um serviço de certificação digital na UFSM, buscando uma solução para a Instituição baseada na problemática existente. O que possibilitará à comunidade acadêmica usufruir de serviços que proporcionem uma maior segurança para seus dados na Internet de modo a satisfazer suas necessidades.

A certificação digital acadêmica é um campo consideravelmente novo que possui vasta área para pesquisa e inovação, exigindo atenção diferenciada dos pesquisadores do ramo. Portanto, são indiscutíveis a atenção e importância que deve-se ter com idéias focadas na atualidade para tirar proveito dessa nova tecnologia de uma forma que venha a contribuir para esta Universidade.

Para atender ao objetivo geral, que é de propor uma possível solução de ICP para a comunidade acadêmica da UFSM, têm-se os seguintes objetivos específicos:

- Estudar conceitos sobre ICPs, seus tipos de hierarquias, políticas de certificação, sobre as entidades que as compõem, bem como suas vantagens e desvantagens;

- Realizar estudos aprofundados sobre o ICP-EDU e seus sistemas desenvolvidos;

- Pesquisar sobre certificados digitais, seu funcionamento, características e formas de gerenciamento;

- Aprofundar conhecimentos no âmbito de assinaturas digitais e autenticação;

- Instalar, configurar, testar e utilizar o Sistema de Gerenciamento de Certificados ICP-EDU (SGCI) e suas respectivas ferramentas complementares.

Este trabalho encontra-se organizado da seguinte maneira: para a revisão de

* Pesquisa parcialmente financiada pelo MEC/SEEP e EAD/UFSM.

literatura têm-se o capítulo 1, onde são apresentados conceitos utilizados em ICPs, seus componentes e entidades. Já, o capítulo 2 diz respeito a certificação digital acadêmica e, também, ao software de gerenciamento de certificados digitais desenvolvido pelo ICP-EDU. O capítulo 3 descreve uma proposta de implementação de uma ICP para a UFSM abordando detalhes da instalação, configuração e testes do SGCI, demonstrando ser esta uma implantação viável para suprir as necessidades da comunidade acadêmica da Instituição. Ainda, neste capítulo, são descritos alguns procedimentos que devem ser realizados e documentos que devem ser formulados para que tal sistema possa ser colocado em funcionamento pleno.

No capítulo 4 encontram-se informações relativas aos resultados obtidos durante o desenvolvimento deste trabalho e também sugestões do que deverá ser implementado em trabalhos futuros. Enquanto que o capítulo 5 dedica-se às dificuldades ocorridas no desenvolvimento deste trabalho e, para encerrar, o capítulo 6 fala sobre as considerações finais fazendo um apanhado geral sobre o trabalho.

1 INFRA-ESTRUTURA DE CHAVES PÚBLICAS

Uma ICP ou *Public Key Infrastructure (*PKI), para Custódio, Graaf e Dahab (2003), é um conjunto de ferramentas e processos para a implementação e a operação de um sistema de emissão de certificados digitais baseado em criptografia de chaves públicas. Engloba também os detalhes do sistema de credenciamento e as práticas e políticas que fundamentam a emissão de certificados e outros serviços relacionados.

Já para a Microsoft (2005) “ICP é um sistema composto de certificados digitais, Autoridades de Certificação (ACs) e outras Autoridades de Registro (ARs) que verificam e autenticam a validade de cada parte envolvida numa transação eletrônica”.

1.1 Certificado digital

Um certificado digital é um documento que contém informações relativas ao seu usuário/proprietário (seja pessoa física, jurídica ou computador), entre elas, a sua chave pública e dados necessários para comprovar sua identidade e também informações como versão, número de série e período de validade. Para garantir sua autenticidade e a veracidade dos dados, o certificado é assinado digitalmente pela autoridade que o emitiu, ligando oficialmente um usuário a uma chave pública, como podemos observar na figura 1, conforme Alecrim (2005). Porém, a aceitação do certificado dependerá dos níveis de confiança dos usuários em relação às práticas e políticas da autoridade que o emitiu.

A solução é trabalhar com delegação de confiança. Nesse processo, segundo a e-Sec (2001), uma entidade confiável, a AC, assina eletronicamente um documento, o certificado digital. Assim o certificado digital tem a chave pública da pessoa e a assinatura da AC. De posse da chave pública da AC qualquer um pode verificar a assinatura do certificado digital e ter certeza que a chave pública contida nele pertence à pessoa nominada no mesmo. Uma vez tendo certeza de que a chave pública do certificado é verdadeira, qualquer pessoa pode verificar a assinatura do proprietário do certificado em qualquer documento eletrônico.

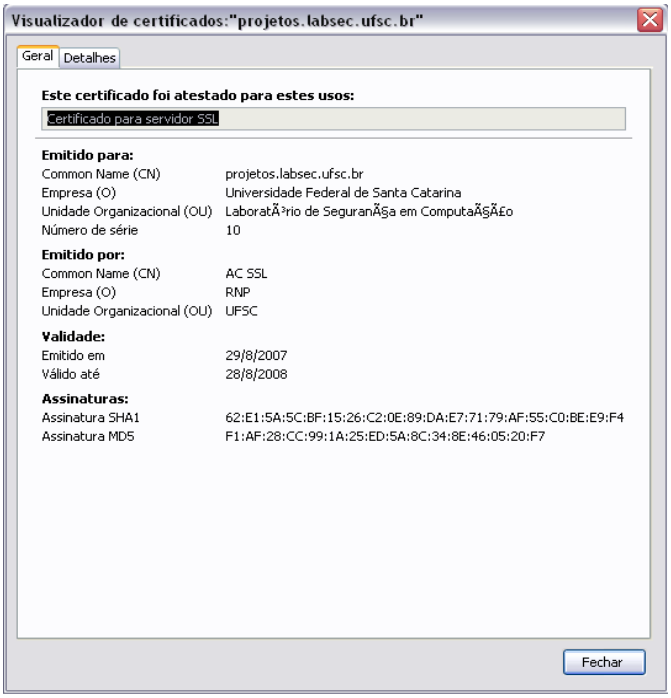

Figura 1 - Exemplo de Certificado Digital

A grande vantagem desse processo é que a AC agora é responsável por identificar a pessoa, receber a sua chave pública e emitir um certificado para ela. Assim, para verificar a assinatura de alguém somente é necessário guardar a chave pública da AC e, sempre que a assinatura de alguém tiver de ser verificada em um documento, a pessoa que verifica precisa apenas do certificado do assinante emitido pela AC. Agora, em vez de o usuário guardar um grande número de chaves públicas no seu computador, somente é necessário guardar a chave pública da sua AC de confiança.

A utilização deste tipo de certificado atualmente vem ganhando importância para garantir a segurança das informações que transitam na grande rede principalmente pelos inúmeros benefícios trazidos, como por exemplo, para realização de transações comerciais eletrônicas que envolvem informações críticas como senhas e números de cartões de crédito.

1.2 Criptografia de chaves públicas

A criptografia constitui-se em um conjunto de métodos e técnicas destinadas a proteger o conteúdo de uma informação, tanto em relação a modificações não autorizadas quanto a alteração de sua origem, sendo uma das técnicas que possibilitam o atendimento dos requisitos básicos de segurança da informação.

STI (1995, apud IGNACZAK, 2002, p. 23) afirma que “o principal objetivo da criptografia é possibilitar a comunicação segura entre duas partes através de um canal não seguro, de tal forma que uma terceira parte não consiga entender o conteúdo que está sendo transmitido”.

Conforme Carlos (2007) a criptografia de chaves públicas ou criptografia de chaves assimétricas tem como base a utilização de duas chaves distintas, uma privada e uma que pode ser mantida pública. Embora sejam complementares, o valor da chave privada não pode ser extraído a partir da chave pública. Para cifrar e decifrar informações, a criptografia assimétrica se dá de forma complementar, onde tudo o que é cifrado com a chave pública só é decifrado com sua respectiva chave privada.

Em relação à algoritmos de criptografia assimétrica, existem dois tipos mais conhecidos. Um deles é o Rivest, Shamir e Adelman (RSA) surgido em 1977 e que atualmente é o mais utilizado. O outro algoritmo é o de assinaturas digitais (*Digital Signature Algorithm*, DSA) que surgiu em 1991 e pode ser usado somente para assinaturas digitais, não podendo ser utilizado para cifragem e distribuição de chaves.

1.3 Funções hash ou funções unidirecionais

Uma função é dita unidirecional ou de hash, para e-Sec (2001), quando possui a característica de transformar um texto de qualquer tamanho em um texto ininteligível de tamanho fixo (têm-se, em média, 20 bytes de saída independentemente do tamanho do texto de entrada). Além disso ela também se caracteriza por ser fácil de calcular e difícil de serem invertidas. Este tipo de função é normalmente usada para efetuar cálculos de integridade de mensagens.

A função é normalmente usada da seguinte forma para cálculo de integridade:

- A partir de uma mensagem qualquer obtém-se o resultado “H” da aplicação da função hash;

- Envia/Armazena-se a mensagem e o resultado “H”.

O processo de verificação de integridade é o seguinte:

- Obtém-se a mensagem e o resultado “H”;

- Calcula-se novamente o resultado “H1” da função hash da mensagem;

- Compara-se H com H1. Se forem iguais, a mensagem está íntegra, caso contrário não.

Atualmente os algoritmos de hash mais utilizados são o Message Digest nº 5 (MD5) e o Standard Hash Algorithm nº 1 (SHA1).

1.4 Assinatura digital

A simples digitalização de uma imagem de alguma assinatura manuscrita não é suficiente para substituir a assinatura manuscrita, pois a mesma pode ser copiada e anexada a qualquer documento tornando-a simples de ser forjada.

Para dificultar o acontecimeto desse tipo de delito, mecanismos de assinatura digital foram criados com o objetivo de substituir a assinatura manuscrita por uma que levasse para o mundo digital as mesmas garantias do mundo real.

O mecanismo de assinatura digital pode ser descrito como uma função hash unidirecional na qual o valor do hash obtido através da aplicação dessa função é em seguida assinado com a chave privada da AC. Nessa assinatura digital, o documento não sofre qualquer alteração e o hash cifrado com a chave privada é anexado ao documento.

> Para comprovar uma assinatura digital são necessários realizar dois passos: descriptografar o bloco de assinatura com a chave pública da AC e executar o algoritmo de função hash no certificado. Se forem iguais, a assinatura está correta, o que significa que foi gerada pela chave privada correspondente à chave pública utilizada na verificação e que o documento está íntegro. Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido alterações no documento ou na assinatura pública (MÜLLER, 2007, p.19).

1.5 Autoridade de certificação - AC

AC é a entidade responsável pela assinatura dos certificados, que são atestamentos feitos por essa AC que diz confiar nestes dados, certificando assim, as chaves públicas dos respectivos proprietários. Eventualmente uma AC também pode ser responsável por outras tarefas como: revogação de certificados, manter informações sobre o status de cada certificado por ela emitido e também emitir listas de certificados revogados.

Certificados revogados são aqueles que não devem mais ser considerados como válidos, pois, embora um certificado tenha uma data de expiração, as vezes é necessário que sua validade seja negada antes do término deste prazo.

Como afirma Carlos (2007), uma ICP pode ser constituída por uma única AC. Porém, em muitos casos, faz-se necessário que determinadas tarefas sejam delegadas à outras entidades a fim de minimizar a carga de tarefas sobre a AC. Por exemplo, uma AC pode delegar à outra AC, denominada AC intermediária, emitir certificados em seu nome ou delegar o processo de identificação dos usuários para uma entidade chamada AR, que será melhor descrita a seguir.

1.6 Autoridade de registro - AR

É responsável por verificar a veracidade das informações apresentadas por alguém que esteja requisitando um certificado digital e também por enviar a requisição do certificado para a AC à qual a AR é subordinada. Através da assinatura da AR, uma AC pode ter certeza que os dados recebidos foram verificados pela AR de sua confiança, conforme Vigil (2007).

2 CERTIFICAÇÃO DIGITAL ACADÊMICA

Com base nos resultados obtidos pelo grupo de trabalho ICP-EDU, que é o pioneiro no País nesse âmbito, têm-se a possibilidade de implantação de uma ferramenta para a proteção da informação em sistemas e serviços que atuam na Internet atendendo aos mesmos requisitos da certificação digital nos moldes comerciais, que é o Sistema de Gerenciamendo de Certificados ICP-EDU (SGCI) e seus respectivos módulos. Pois, apesar da Internet ser um recurso de comunicação que possibilita uma fácil manipulação de grandes volumes de dados independente da localização geográfica, muitas vezes a rede faz com que as informações circulem de forma vulnerável e, como dito, em certos casos há a necessidade de que estas informações trafeguem inacessíveis para usuários mal intencionados.

2.1 SGCI - Sistema de Gerenciamento de Certificados ICP-EDU

No ano de 2001, a ICP-Brasil foi reconhecida legalmente através da instituição da Medida Provisória nº 2.200-2, segundo Lins (2005). Antes disso, para Custódio (2005), no Brasil, a forma de distribuição e publicação de chaves públicas podia ser feita livremente em qualquer lugar, de forma idêntica a uma lista telefônica. Bastava que um usuário solicitasse a inclusão de sua chave em um diretório público. Esta era uma forma eficiente de se obter a chave pública de alguém, porém, sem nenhum tipo de segurança, pois não existia ligação entre a chave enviada para o diretório e o usuário que a enviou.

Os certificados digitais, como dito anteriormente, surgiram para sanar este problema, pois ligam oficialmente um usuário a uma chave pública. Porém, isso não é o bastante devido à necessidade de alguma forma de gerenciamento desses certificados.

A ferramenta SGCI foi desenvolvida para atender a necessidade de suportar uma infra-estrutura de gerenciamento de todo o processo de criação, ciclo de vida e revogação de certificados digitais. Ela é distribuída de forma totalmente gratuita, possibilitando, assim, que as instituições de ensino e seus usuários também possam usufruir dessa nova tecnologia.

2.1.1 Estrutura do SGCI

O SGCI encontra-se dividido em 3 componentes funcionais básicos, apresentados na figura 2, que são: O sistema gestor, o módulo público e o diretório público.

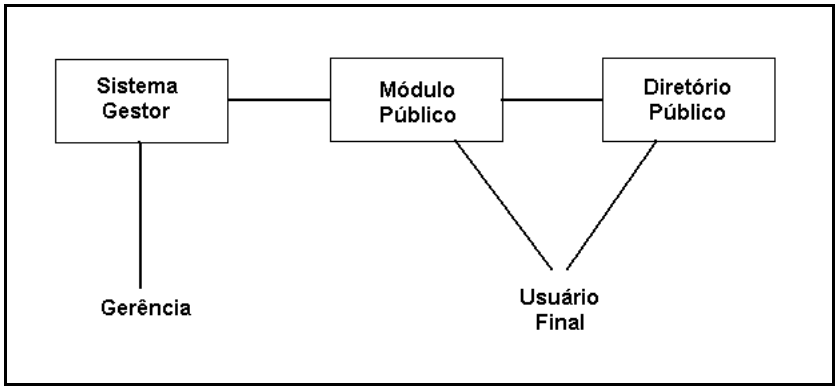

Figura 2 - Estrutura do SGCI

O sistema gestor engloba funções de apoio necessárias ao funcionamento de uma Infra-estrutura de Chaves Públicas (ICP), assim como a criação e gerenciamento de Autoridades Certificadoras (ACs) e de Autoridades de Registro (ARs), afirma Custódio (2005).

O Módulo Público (MP) e o Diretório Público (DP) destinam-se aos usuários finais, pois o primeiro possibilita o fornecimento de certificados através de solicitação, que deve ser feita entrando em contato pessoalmente com o Operador responsável para a comprovação de dados, conforme determinado pelas políticas de certificação da ICP. Enquanto o outro consiste em um banco de dados de certificados válidos e uma Lista de Certificados Revogados (LCR).

No caso do SGCI, seu MP possibilita a emissão de certificados digitais para serem utilizados em servidores *web,* ou seja, este MP tem como usuário final este tipo de aplicação específica. Entretanto, seu DP é destinado a qualquer indivíduo que queira confirmar a veracidade de um certificado ditigal emitido pela respectiva AC através do *download* da LCR.

Pode-se averiguar quando um servidor *web* faz uso de um certificado digital ao acessar uma *home page* hospedada no mesmo. Ao realizar o acesso, verifica-se que ela apresenta um ícone no formato de um cadeado, o qual normalmente encontra-se no canto inferior direito do navegador de Internet, como é possível

observar na figura 3. Ao clicar neste ícone, será apresentada uma tela na qual estarão dispostos todos os dados que compõem tal certificado.

Figura 3 - Verificando a existência de um certificado digital

Os navegadores de Internet mais usuais, como por exemplo o Firefox, o Internet Explorer e o Opera, já possuem embutidos os certificados digitais da maioria das Autoridades Certificadoras Raiz conhecidas mundialmente. E, ao acessar uma *home page* que tenha um certificado digital assinado por uma AC subordinada a alguma dessas ACs-Raiz, têm-se a verificação da veracidade do certificado digital realizada automaticamente.

No caso da UFSM, que terá sua própria AC-Raiz, ao acessar pela primeira vez uma *home page* que possua um certificado emitido por alguma AC subordinada que faça parte desta ICP, será exibida uma tela no navegador questionando o usuário sobre o que ele deseja fazer com o certificado digital que a *home page* acessada por ele possui, como mostra a figura 4.

Figura 4 - Primeiro acesso a um *site* com certificado digital desconhecido

A partir daí, para verificar a veracidade do certificado, basta comparar a assinatura digital da AC que é apresentada no certificado com a assinatura da mesma AC que encontra-se disponível no DP. Vale ressaltar que este procedimento é valido para quando se está utilizando qualquer tipo de certificação digital e não apenas para o uso da certificação digital acadêmica.

Como observa-se, estes MP e DP atendem somente usuários finais do tipo servidor *web*, no entanto, conforme será visto mais adiante, existe um ferramenta complementar ao SGCI que disponibiliza outro MP que atua como interface para emissão de certificados com outra finalidade e outro perfil de usuário final.

2.1.2 Módulo de *hardware* seguro

O grupo de trabalho eleito pela Rede Nacional de Ensino e Pesquisa (RNP) desenvolveu o Módulo de *Hardware* Seguro ou *Hardware Secure Module* (HSM). O grande desafio que foi lançado na produção desse *hardware* e posteriormente alcançado era que seu custo final ficasse por volta de U$1.000,00.

Ele é um protótipo que, além de atuar como acelerador criptográfico, podendo chegar a realizar centenas de assinaturas por segundo com a chave privada que protege, possui a finalidade de propiciar uma transmissão de dados realmente segura para sistemas de gerenciamento de certificados, isto é, possibilita a gestão segura do ciclo de vida de chaves privadas.

No caso de uma AC, conforme a RNP (2006a), a função de um HSM é servir como “cofre” para a chave privada de assinatura de certificados digitais e não há como acessá-lo, a não ser pela sua interface padrão.

Atualmente o sistema de gerenciamento de certificados acadêmico encontra-se em uso na Universidade Federal de Santa Catarina (UFSC) e o desenvolvimento do HSM, apresentado na figura 5, está em seu início de produção em maior escala, para que possa ser fornecido às instituições de ensino interessadas em futuramente fazer parte da ICP que está sendo implantada pela RNP, pois para isso as universidades precisariam acoplar aos seus sistemas tal equipamento, segundo a RNP (2007).

Figura 5 - Módulo de *hardware* seguro

3 CERTIFICAÇÃO DIGITAL ACADÊMICA - PROJETO E PROPOSTA DE IMPLANTAÇÃO NA UFSM

A Rede Nacional de Ensino e Pesquisa já possui inaugurada e em funcionamento sua AC-Raiz, que é a entidade de mais alto nível na hierarquia dessa Infra-estrutura de Chaves Públicas e a qual as instituições pertencentes ao ICP-EDU atualmente são subordinadas, pois possuem seus respectivos Módulos de *Hardware* Seguro, um dos quesitos primordiais para que seja efetivada tal subordinação. O objetivo seguinte da RNP (2006b) é, a partir de 2008, abrir espaço para que outras Instituições de Ensino Superior interessadas possam fazer parte da ICP da RNP. Com isso pretende-se que a UFSM esteja com sua ICP em pleno funcionamento até o início do próximo ano para, assim que possível, ter sua Autoridade Certificadora Raiz ligada à RNP.

O trabalho, na UFSM, concentrou-se na implantação de uma AC-Raiz local através da instalação, configuração, testes do SGCI, além de estudos sobre políticas de governança de certificados. Para que, assim que sejam liberados os novos HSMs, a Instituição possa adquirir tal equipamento, já possuindo sua ICP em funcionamento, e possa, então, subordinar-se à infra-estrutura da RNP.

Nesse sentido, serão descritos a seguir relatos do que foi conseguido até o presente momento nesta Instituição.

3.1 SGCI - Modos de obtenção

Encontram-se duas opções relativas à estrutura pela qual se pode obter o SGCI a partir da *home page* do Laboratório de Segurança em Computação (LabSEC) - Laboratório pertencente à UFSC que, como dito, faz parte do grupo de pesquisa responsável pelo desenvolvimento do SGCI. A primeira opção direciona para uma estrutura uniforme, na qual se instala todo o sistema a partir de um único pacote, chamado de Pacote de Certificação Digital (PCD).

O PCD é um conjunto de programas contendo, além do sistema operacional, que é o OpenBSD, o próprio SGCI com o MP e o DP, um servidor *web* Apache com suporte a SSL, *Webmail* seguro e também o banco de Dados PostgreSQL. O

OpenBSD é distribuído em código fonte sem custos, o que o torna uma boa opção para redução de gastos principalmente em se tratando de sistemas desenvolvidos no meio acadêmico. Além disso, ele é considerado por muitos profissionais de segurança como um dos mais seguros sistemas operacionais existentes na atualidade, afirma OpenBSD (2004), o que, obviamente, vem muito a calhar quando se trata da sua utilização em sistemas que envolvam segurança da informação, como é o caso do SGCI.

A segunda opção leva a uma estrutura dividida em módulos, na qual o SCGI pode ser obtido separadamente do MP e do DP e instalado em alguma distribuição do sistema operacional Linux - não existe a opção de utilização de alguma versão do sistema operacional Windows - contudo, devemos ter previamente instalados e configurados o servidor *web* Apache2 com suporte à PHP e SSL e também o banco de dados PostgreSQL em versão 8 ou superior. Existe a possibilidade de instalação de dois outros complementos, um chamado de Assinador, que possui a finalidade de propiciar assinaturas digitais utilizando o HSM e outro chamado de Libcryptosec, que é uma biblioteca criptográfica utilizada em conjunto com o Assinador para dar suporte a outras funções criptográficas, *SmartCards* e afins.

Todavia, independentemente das opções de instalação, tal processo não se dá de forma trivial e automatizada, exigindo razoáveis conhecimentos em configuração do sistema operacional utilizado e também do banco de dados e servidor *web*.

No trabalho desenvolvido na UFSM optou-se pela segunda opção, pois pelo histórico de versões encontradas para *download* na *home page* que disponibiliza o sistema, observou-se que esta opção possui atualizações mais freqüentes do *software* em comparação à primeira. No caso, quanto ao sistema operacional, foi escolhido o Linux, em sua distribuição Debian Etch, para a instalação do SGCI, como será abordado em mais detalhes a seguir.

3.2 Organização operacional do SGCI

A organização dos operadores do sistema é feita através da atribuição de papéis, os quais estão estruturados de forma hierárquica. O acesso aos recursos do ambiente é dependente do papel atribuído ao operador, onde o Criador é o

responsável pela criação de entidades ACs, ARs e associação de usuários ao papel de Administrador. Os Administradores têm poderes para alterar configurações das entidades criadas e associar usuários ao papel de Operador. Por sua vez, os Operadores têm permissão para emitir/revogar certificados e também avaliar requisições de novos certificados, como podemos observar na figura 6. Aos usuários finais cabe a solicitação de certificados e consultas sobre status de certificados no módulo público e diretório público respectivamente.

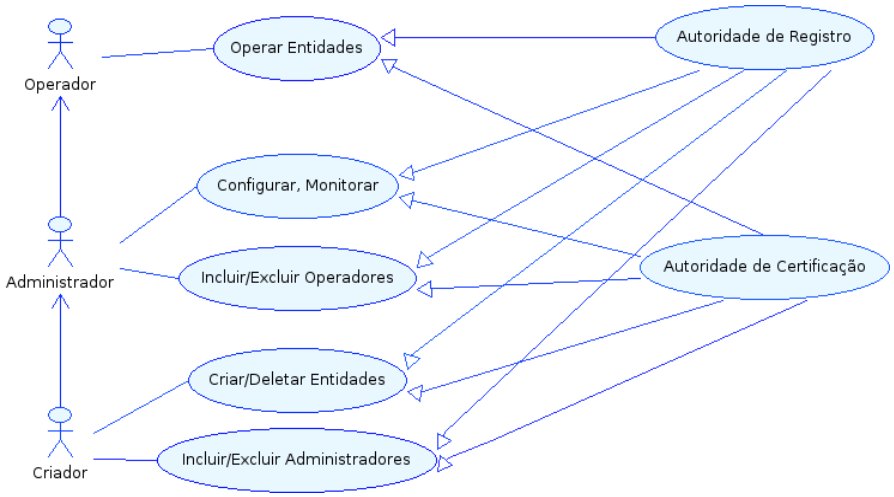

Figura 6 - Diagrama de casos de uso: Organização operacional

3.3 Autoridade Certificadora de Correio Eletrônico

No caso da implantação do serviço de emissão de certificados para a comunidade acadêmica da UFSM, inicialmente tem-se a intenção de disponibilizar para estes usuários, certificados digitais com restrição de uso. Ou seja, em uma primeira fase serão emitidos apenas certificados para uso em correio eletrônico, não sendo possível usá-los para autenticação em servidores.

Portanto, nesse caso, o módulo público que será disponibilizado é uma entidade que compõe uma outra ferramenta chamada de Autoridade Certificadora de Correio Eletrônico (AC-Correio) e é através dela que poderá ser feito o acesso ao módulo público de forma fácil por quem deseja formalizar uma requisição de certificado para uso em correio eletrônico.

Dessa forma, na UFSM, teremos duas categorias de usuários finais. Refere-se, aqui, usuários finais àqueles que podem possuir um certificado digital.

A primeira é a categoria dos servidores *web*, na qual o responsável pelo

servidor, que julgar necessário que seu equipamento utilize-se da tecnologia, deverá entrar em contato, como dito anteriormente, pessoalmente com o responsável da Autoridade Certificadora. Assim, após obtido e instalado o certificado digital no servidor, os clientes que acessarem as *home pages* hospedadas nele poderão ter a certeza de que o *site* é legítimo, pois o certificados digitais para servidores *web* identificam os servidores e impedem que seus usuários sejam enganados por *sites* clonados ou fraudados, conforme explicado na seção 2.1.

A outra é a categoria da comunidade acadêmica da UFSM em geral, na qual enquadram-se alunos, professores, servidores, entre outros, que, para possuírem um certificado digital, necessitam acessar o Módulo Público da AC-Correio, como será explicado com mais detalhes a seguir.

3.3.1 Requerendo um certificado para uso em correio eletrônico

Os interessados em obter um certificado digital devem ser membros da comunidade acadêmica da UFSM, seja na forma de alunos da graduação, alunos da pós-graduação, servidores ou docentes. Bem como devem possuir um endereço eletrônico de *e-mail* de pelo menos um dos seguintes domínios: ufsm.br, cpd.ufsm.br ou inf.ufsm.br, pois existe um arquivo de configuração da AC-Correio que permite a retirada/inclusão de possíveis domínios de *e-mail* permitidos para emissão de certificados. Logo, como medida restritiva, fazendo com que somente a comunidade acadêmica da UFSM tenha possibilidade de obter um certificado digital, inicialmente foram inclusos apenas os três domínios citados acima.

A partir desses pré-requisitos, os interessados devem acessar a URL da AC-Correio que será divulgado e apenas preencher o formulário com seu endereço de *e-mail* de um dos domínios mencionados. Nesse instante, como forma de autenticação do requerente do certificado, será enviada uma mensagem para o *e-mail* fornecido contendo um desafio-resposta, o qual só poderá ser respondido pela pessoa que detem as informações corretas. Após completados esses passos, a AC-Correio enviará o certificado digital para o *e-mail* fornecido.

Uma informação que deve ser ressaltada quanto ao uso de certificado digitais para correio eletrônico é que atualmente não existe nenhum *webmail* que dê suporte à utilização de tais certificados. Para usufruir dessa tecnologia precisa-se ter

instalado um *software* cliente de *e-mail,* tal como Outlook Express ou Mozilla Thunderbird, através do qual importa-se o certificado emitido para que se possa assinar digitalmente as mensagens a serem enviadas.

3.3.2 Objetivo da AC-Correio

Outro dado relevante que deve ser citado é o motivo pelo qual utiliza-se a Autoridade Certificadora de Correio Eletrônico ao invés do próprio SGCI para a emissão de certificados para o uso em correio eletrônico. A AC-Correio foi concebida com o objetivo de agilizar o processo de emissão de certificados. A idéia dela é simples: requisição submetida, certificado emitido.

Esta agilidade pode acontecer pelo fato de não existir, na AC-Correio, a entidade da Autoridade de Registro a qual, como afirmado anteriormente, possui a função de verificar se os dados de quem está requerendo um certificado são verdadeiros. Isso torna-se possível através da restrição da emissão de certificados somente para aqueles que possuem uma conta de *e-mail* pertencente à UFSM e, por terem tal conta, a Instituição, de antemão, já possui os dados pessoais de tal indivíduo, como por exemplo, nome e matrícula, associados ao endereço de *e-mail*.

Ou seja, por não existir a necessidade de verificação dos dados do requerente de um certificado para uso em correio eletrônico, o processo de emissão do respectivo certificado torna-se muito mais ágil.

3.4 Hierarquia das entidades

Quando trata-se de pequenos ambientes, como, por exemplo, pequenas empresas onde o volume de certificados emitidos é pequeno, normalmente, opta-se pela adoção de uma hierarquia simples composta por somente uma AC, a qual gerencia e toma todas as medidas cabíveis para o funcionamento normal da ICP.

Contudo, não se sabe como será a demanda da comunidade acadêmica da UFSM por certificados digitais. Porém, assim como se prevê que o uso desta tecnologia irá aumentar significativamente em um futuro próximo, as expectativas para a Instituição são de que exista uma demanda considerável, o que exige maior complexidade na organização hierárquica das entidades, ou seja, uma forma mais modularizada e subdividida para dar suporte a essa demanda.

Nesse caso, já prevendo um volume maior de certificados a serem gerenciados futuramente e também levando como referência aspectos da organização hierárquica existente atualmente da ICP-Brasil e da ICP-EDU, optou-se, na UFSM, por uma estrutura divida em níveis hierárquicos onde possui-se uma AC-Raiz, que não emitirá certificados para usuários finais mas que o fará para outras ACs chamadas de subordinadas. Estas últimas é que possuem tanto a possibilidade de emitirem certificados para que outras ACs subordinadas abaixo na hierarquia quanto a finalidade de fornecer o serviço para os usuários finais.

Dessa maneira o usuário utilizador do certificado digital possui um único ponto de confiança que é a AC-Raiz, porém, conseqüentemente, ele passa a confiar nas ACs subordinadas à AC-Raiz, já que elas foram certificadas inicialmente pelo ponto mais alto da hierarquia. A figura 7, abaixo, exemplifica essa idéia de hierarquia e relação de confiança entre entidades.

Essa forma de organização permite a criação de ACs ou ARs subordinadas conforme exista demanda pelo serviço na Instituição.

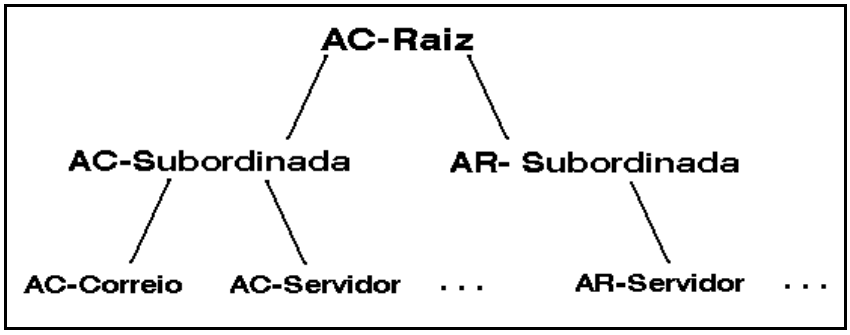

Figura 7 - Exemplo de hierarquia da ICP-UFSM

3.5 Declaração de práticas de certificação

Toda a ICP deve possuir um documento chamado de declaração de práticas de certificação, que por sua vez deve ser disponibilizado de maneira fácil a qualquer indivíduo interessado de forma anônima.

Este documento, disponível no repositório da ICP-EDU a título de pesquisa, é muito detalhado e trata sobre a especificação dos procedimentos empregados na execução dos serviços oferecidos pelas entidades que compõem uma ICP. Como, por exemplo:

- Quais são os possíveis usos para um certo certificado (se ele pode ser

usado para autenticação em servidores *web* ou apenas para correio eletrônico);

- Informações sobre responsabilidades referentes a publicações e repositórios;
- Requisitos operacionais do ciclo de vida do certificado (quem pode submeter uma solicitação de certificado, processo de solicitação e responsabilidades, emissão, revogação e renovação de certificados, etc);
- Controles de segurança física (acesso físico, armazenamento de mídia, energia e refrigeração, etc).

Dessa forma, como trata-se de um documento complexo que especifica todos as responsabilidades e procedimentos adotados por uma ICP, cabe não somente a uma pessoa elaborá-lo. Mas sim, deve-se nomear um ou mais comitês para fazê-lo com a finalidade de formar um modelo de governança, como é o que acontece em outras instituições, caso deseje-se ter uma ICP local funcionando em plenas condições. Assim, como um trabalho de graduação é elaborado por um autor, as orientações devem ser discutidas pelos comitês a serem formalizados na UFSM. Mais detalhes relativos a esse assunto serão abordados no tópico a seguir.

3.6 Modelo de governança

Quanto trata-se da designação de responsabilidades sobre a operação de uma Infra-estrutura de Chaves Públicas, bem como sobre quem deve responder por eventuais incidentes que venham a acontecer, utiliza-se um modelo de governança.

A criação de um modelo de governança dá-se através da formação de um grupo de indivíduos que geram o chamado Comitê Gestor. O Comitê Gestor é responsável pela criação de outros grupos de pessoas chamados de Grupos de Operação e pela formulação do documento chamado de Práticas de Certificação.

Por sua vez, estes Grupos de Operação são responsáveis por funcionalidades como operacionalização tanto de suas respectivas entidades quanto das entidades subordinadas realizando os procedimentos especificados no documento de Práticas de Certificação, tais como:

- Criar e armazenar a chave privada;

- Manter uma cópia de todas as requisições de certificados;
- Receber requisições aprovadas da AR Raiz para a emissão de certificados às ACs intermediárias;
- Emitir, publicar e revogar certificados digitais;
- Nomear os administradores e operadores para as ACs.

Como observou-se na ICP-EDU, é comum a criação de um Grupo de Operação que seja responsável pela a AC-Raiz e outro pela a AR-Raiz que façam parte da ICP local.

No caso da implantação de uma ICP na UFSM, tais procedimentos deverão ser realizados para consolidar o interesse de que esta ICP, em um futuro próximo, faça parte da ICP-EDU, da RNP, que estará vinculando ICPs de novas IES que ainda não fazem parte dessa infra-estrutura a partir do ano de 2008.

4 RESULTADOS E DIFICULDADES ENCONTRADAS

4.1 Preparando o ambiente para a instalação do SGCI no servidor *web* da UFSM

Como descrito na seção anterior, o sistema operacional escolhido para a instalação do SGCI e seus complementos foi o Debian em sua versão mais atual, que é a 4.0. Esta é uma distribuição Linux muito utilizada para hospedagem de servidores no mundo todo, pois é considerada uma distribuição muito estável o que a torna bastante eficiente quando deseja-se ter um funcionamento do sistema ininterrupto pelo maior tempo possível.

A instalação foi efetuada de modo simplificado, incluindo apenas os pacotes de *softwares* básicos para o funcionamento do sistema como servidor.

4.1.1 Instalação e configuração do servidor *web*

Serão descritos a seguir, sucintamente, os passos realizados para a instalação e configuração do Apache 2 de forma a propiciar o seu correto funcionamento em conjunto com o SGCI. Não serão abordados detalhes aprofundados de configuração porque acredita-se que isto tangencia o foco principal deste trabalho.

No Debian, o Apache 2 pode ser obtido e instalado de maneira fácil apenas digitando-se o comando “apt-get install apache2”. Após realizado esse primeiro passo, passa-se para a configuração do servidor. Em sequência, deve-se editar o arquivo “ports.conf” que encontra-se no diretório “/etc/apache2” onde devem ser incluídas as linhas contendo o nome do servidor e a porta que será utilizada, como no exemplo:

```
ServerName icpufsm.cpd.ufsm.br
Listen 8080
```

A seguir deve-se incluir um novo arquivo referente ao *site* do SGCI no diretório “/etc/apache2/sites-available” e, após isso, fazer as modificações necessárias no arquivo para que o novo *site* possa funcionar corretamente.

Por final, basta incluir um link simbólico no diretório “/etc/apache2/sites-enabled” referenciando o *site* criado no diretório anterior, criar um diretório dentro do

diretório “/var/www” com o mesmo nome do arquivo que foi criado dentro do diretório “sites-available” e reiniciar o Apache2.

4.1.2 Instalação e configuração do banco de dados

O PostgreSQL é um sistema gerenciador de banco de dados (SGBD) objeto-relacional, ou seja, implementa, além das características de um SGBD relacional, algumas características de orientação a objetos, como herança e tipos personalizados, conforme PostgreSQLBR (2006). O qual afirma ainda que ele é um sistema robusto, confiável, seguro e que possui recursos comuns a bancos de dados de grande porte, mesmo sendo de código-fonte aberto.

A obtenção e instalação deste banco de dados se dá de forma similar ao servidor web e o comando é o que segue: “apt-get install postgresql-8.1”.

4.1.3 Instalação do SGCI

Antes da instalação propriamente dita do SGCI, alguns pacotes referentes ao servidor *web* e o sistema de banco de dados devem ser instalados para dar suporte ao correto funcionamento da ferramenta. São eles: curl, libapache2-mod-php5, libp11-dev, libapache2-mod-auth-pgsql, php5-curl, php5-pgsql.

Além disso, devem ser instalados os respectivos complementos citados anteriormente neste trabalho que acompanham o SGCI: o Assinador e a Libcriptosec. Para a obtenção dos complementos deve-se acessar a *home page* do LabSEC, através do seguinte *link*: http://projetos.labsec.ufsc.br. Após o *download* dos arquivos, digita-se, para cada um deles, o comando “dpkg -i nome-do-arquivo.deb” para efetivar a instalação dos mesmos.

Em sequência, o arquivo do SGCI deve ser descompactado dentro do diretório criado em “/var/www”, conforme descrito na seção anterior que trata do servidor *web,* e os seguintes comandos executados:

```
$ cd /var/www/diretorio-criado
//criando a base de dados
$ su -l postgres -c "createdb -E latin1 icpedu"
//criando as tabelas da base de dados
$ su -l postgres -c "psql -d icpedu -f /var/www/html/sgci/create.sql"
```

```
//criando o usuário
$ su -l postgres -c "createuser icpedu -P"
$ Enter password for new role:
$ Enter it again:
$ Shall the new role be a superuser? (y/n) y
```

Após, deve-se editar o arquivo responsável pela autenticação de usuários, que é o “pg_hba.conf” e se encontra no diretório “/var/lib/pgsql/data”. Nele, deve-se inserir as seguintes linhas:

```
local   icpedu      icpedu                          md5
host    icpedu      icpedu        127.0.0.1/32      md5
```

Em seguida, deve-se dar permissão de escrita ao PostgreSQL em algumas pastas do sistema. As pastas são:

- ac/arquivos
- ar/arquivos
- engines
- temp
- publico/arquivos
- log

E o comando é: “chown -R www-data:www-data /var/www/html/nome-do-diretorio”. Após a realização destes passos reinicia-se o serviço do PostgreSQL com o comando “/etc/init.d/postgresql restart”, a instalação estará concluída e poderemos visualisar a interface inicial, conforme a figura 8, digitando no *browser* o IP do servidor seguido de “/sgci”. Não se deve esquecer de alterar o arquivo lib/dblayer.inc.php ajustando o valor da variável $password para a senha do usuário criado no processo de instalação do sistema, quando foi criado o usuário do banco de dados.

A partir desse momento pode-se verificar a interface gráfica da ferramenta. Ela é amigável e seu uso é simples e fácil desde que os operadores possuam um conhecimento prévio do potencial da ferramenta em relação às suas funcionalidades, como por exemplo, os campos que dizem respeito ao período de validade dos certificados, ao tamanho das chaves (quantidade de bits) geradas para o certificado, ao algoritmo a ser utilizado e aos usos permitidos do certificado.

Figura 8 - Tela inicial após a instalação do SGCI

4.2 Módulo público - Instalação e configuração

O módulo público é a ferramenta desenvolvida a fim de possibilitar contato direto com o usuário final. É através dele que os interessados em solicitar um certificado digital devem proceder para gerar uma requisição de certificado.

Inicialmente deve-se realizar a preparação do banco de dados para que o módulo público possa funcionar de forma correta. Para isso, deve-se instalar o suporte ao Qt4 (é uma biblioteca de classes em C++ que possui funcionalidades relativas à XML e banco de dados) através do comando “apt-get install lsb-qt4 libqt4-sql” e também a biblioteca PHP Pear digitando no terminal “apt-get install php-pear”.

Em seguida, o próximo passo é descompactar o arquivo relativo ao MP no diretório “/var/www/” do servidor *web*, configurar o arquivo php.ini, que se encontra em “/etc/php5/apache2” incluindo a seguinte linha “include_path= ".:/var/www/modulo-publico/lib"” na seção relativa a *paths* e *directories.*

Logo após, deve-se criar os links simbólicos dos arquivos pgsql.so, pdo.so e pdo_pgsql.so que estão no diretório “/usr/lib/php5/200xxx” para a pasta “/usr/lib/php5”. Para isso, temos que digitar o sequinte comando: “ln -s /usr/lib/php5/200xxx/nome-do-arquivo /usr/lib/php5”

Finalmente, basta reiniciar o serviço do servidor *web* através da seguinte instrução “/etc/init.d/apache2 restart” para que a ferramenta possa começar a ser utilizada.

4.3 Autoridade Certificadora de Correio Eletrônico - Instalação e Configuração

A AC-Correio, é dividida em duas entidades: o servidor de serviços criptográficos e o módulo público. O primeiro, trabalha consumindo requições e emitindo certificados e lista de certificados revogados. O segundo é uma aplicação *web*, pela qual usuários podem gerar requisições de certificados digitais e listas de certificados revogados.

Para iniciar a instalação do servidor criptográfico, após obter o arquivo a partir da *home page* do LabSEC, conforme o link mencionado anteriormente, deve-se executar o comando “mail-ca-server/Makefile”. Em seguida, tem-se que criar um usuário, uma base de dados e um esquema para a base de dados no PostgreSQL.

Para criar o usuário primeiro é necessário logar-se como administrador do banco de dados através do comando “su postgres” e, após, para efetivamente criar o usuário, digitar o comando “createuser -P nome-do-usuário”. Já, para criar a base de dados o comando “createdb -h localhost -U nome-do-usuário -O nome-do-usuário nome-do-usuário” deve ser inserido. Por final, para criar o esquema da base de dados, digita-se a instrução “psql -h localhost -U icpedupiloto -f tables.sql”.

Em seguida, deve-se alterar a linha “<password>senha<passord>” no arquivo “caserv.xml” inserindo a senha do usuário criado no início deste procedimento. Por último, para iniciar a execução do serviço basta escrever o seguinte comando “mail-ca-server/mail-ca-server”.

O Módulo Público deve ser instalado, após o arquivo obtido através *da home page* do LabSEC ser descompactado, através do comando “unzip modulo-publico-xxx.zip”, a partir da configuração do arquivo “php.ini” que encontra-se no diretório “/etc/php5/apache2”. Deve ser localizada, neste arquivo, a seção que referência “Paths and Directories ” e incluso o caminho do diretório “lib”, o qual se encontra no diretório do modulo-publico que foi descompactado, como o exemplo que segue: include_path= ".:/var/www/modulo-publico/lib"

Em seguida o comando “apt-get install php-pear ” deve ser executado e os links simbólicos dos arquivos “pgsql.so”, “pdo.so” e “pdo_pgsql.so ” devem ser criados. Tais arquivos encontram-se no diretório “/usr/lib/php5/200...” e seus links deverão ser criados em “/usr/lib/php5”, através do comando “ln -s /usr/lib/php5/200.../nome-do-arquivo /usr/lib/php5”.

Para finalizar, a tarefa é adicionar os domínios que podem solicitar certificados no arquivo conf/publicModule.xml e reiniciar os serviços do banco de dados e servidor *web* através do comando “/etc/init.d/apache2 postgresql restart”.

Logo após o processo de instalação da AC-Correio, a tela inicial apresenta as três ações que os usuários podem ter, conforme apresentado na figura 9.

Figura 9 - Autoridade certificadora de certificados de correio eletrônico

4.4 Testes, expectativas e dificuldades

Pôde-se constatar, através da realização de muitos testes, que, tanto o Sistema de Gerenciamento de Certificados ICP-EDU, quanto a ferramenta que o complementa, a Autoridade de Correio Eletrônico, corresponderam muito bem às expectativas relativas ao gerenciamento do clico de vida dos certificados digitais, ou seja, à emissão/revogação de certificados e emissão de listas de certificados revogados. Outros requisitos, como a criação de Autoridades Certificadoras e Autoridades de Registro para estruturar uma hierarquia de entidades e a criação de usuários para a administração do sistema associando-os aos seus respectivos papéis, também transcorreram como esperado.

Foram feitos testes de emissão/revogação de certificados, tanto no âmbito de servidores como no de correio eletrônico. Também foram realizados experimentos quanto à hierarquia da Infra-estrutura de Chaves Públicas através da criação/extinção tanto de ACs como de ARs. A construção da hierarquia deu-se através da importação pela(s) AC(s) de nível inferior na hierarquia dos certificados emitidos pela AC de nível superior, bem como a realização das ligações entre ACs e ARs de modo que estas últimas saibam a quais ACs devem encaminhar suas respectivas requisições.

Em relação à administração e gerência do sistema como um todo, que, foi feita através da associação de indivíduos a papéis, o *software* comportou-se

exatamente como relatado neste trabalho, sendo que cada indivíduo teve permissão para executar exatamente as operações associadas ao seu papel.

Quanto a trabalhos futuros, no momento está-se na expectativa da decisão da Rede Nacional de Ensino e Pesquisa sobre qual rumo seu projeto da ICP irá seguir no que diz respeito à adesão de outras Instituições de Ensino Superior a esta ICP, para que em breve a UFSM possa fazer parte da lista de IESs ligadas à ICP da RNP.

Outra tarefa que merece destaque é a criação do comitê gestor e dos grupos de operação. A criação de tais grupos é necessária como medida para tornar público os nomes dos responsáveis pelo funcionamento da ICP-UFSM como um todo, bem como para elaborar os documentos que contenham os detalhes sobre as práticas e políticas necessárias, já citadas anteriormente. Estas serão tomadas como base para decisões futuras e também para dar início a operação da AC-Raiz da UFSM.

O início do funcionamento dessa AC-Raiz será marcado por muitos procedimentos, como apresentado no capítulo 3, sendo que todos eles deverão ser realizados com a presença de testemunhas e documentados por meio de cerimoniais, que descreverão, entre outras informações, todos os passos para geração do par de chaves criptográficas do certificado digital AC Raiz, o qual será auto-assinado.

Dessa forma, todo o processo de implantação do sistema dar-se-á de maneira mais transparente possível, fazendo surgir, de forma natural, uma relação de confiança entre os usuários, a ICP-UFSM e seus certificados emitidos.

Quanto às dificuldades encontradas, como normalmente acontece com a utilização de ferramentas novas ou que ainda estão sofrendo constantes aperfeiçoamentos, um dos grandes obstáculos é encontrar documentação sobre as mesmas.

No caso do SGCI e da AC-Correio não foi diferente e esta foi a maior dificuldade encontrada. Estes são softwares ainda em fase de amadurecimento e por isso a documentação relativa à instalação ou configuração é extremamente precária e, quando existe, algumas vezes é contraditória devido à disponibilização de forma assíncrona das versões dos softwares e suas respectivas documentações. Nesse sentido, ocorreu um esforço extra para que fosse possível a obtenção dos resultados conseguidos até o momento e tais fatos foram encarados de forma

normal devido ao entendimento de que este trabalho possui caráter inovador.

Por final, outra dificuldade foi a de não se obter maiores informações de quando será possível, quais as medidas a serem tomadas e de que forma será feita a inclusão da ICP local da Instituição à ICP que está em operação sob domínio da RNP através de uma relação de confiança.

5 CONSIDERAÇÕES FINAIS

A certificação digital é uma assinatura virtual que torna mais segura a prática de atividades *on-line*, como por exemplo o uso de *Internet banking* em transações bancárias, onde o banco terá a certeza de que quem está acessando a conta corrente é realmente o cliente responsável por ela.

Por essa importância e por todos os outros benefícios citados anteriormente, tentou-se, aqui, expor um panorama da situação atual da certificação digital acadêmica e o que está sendo realizado na UFSM, abordando sobre os trabalhos que têm sido desenvolvidos na área acadêmica e já utilizados em ambientes de algumas instituições universitárias brasileiras.

A ICP de âmbito educacional pode funcionar como grande aliada da UFSM e de seus usuários, auxiliando o ambiente acadêmico, pois este utiliza um tráfego digital de informações importantes, como históricos escolares, resultados de pesquisas, notas de provas, informações administrativas, informações financeiras, etc. Ela traz, nesse panorama, a otimização de processos, ou seja, a disponibilização de serviços com maior agilidade e menor burocracia, oferecendo ainda maior segurança.

Outra vantagem, dentre as que podem ser citadas, é a substancial redução de custos possibilitada pela desmaterialização dos processos através do uso de documentos digitais, acarretando, além de grandes economias com gastos em papel, uma agilidade segura no trâmite de documentos.

Por fim, atualmente a maioria das universidades brasileiras, para poderem contar com uma assinatura digital válida e de confiança, necessitam recorrer a instituições privadas. Então, unicamente se tratando de certificação digital acadêmica, os benefícios em relação a custos são ainda maiores, pois estes se restringem apenas à instalação e à disponibilização do serviço para a comunidade acadêmica em geral, para a qual o serviço é ofertado gratuitamente.

Neste trabalho foram realizados estudos sobre certificados digitais, no que diz respeito às suas características, modos de utilização, benefícios e desvantagens. Também foram explorados conceitos sobre criptografia de chaves públicas, mecanismo de assinatura digital e possibilidades de implantação de uma ICP local,

onde optou-se pela utilização de um sistema de gerenciamento de certificados digitais, o SGCI, idealizado pelo grupo de trabalho ICP-EDU.

Pesquisas foram desenvolvidas relativas às formas de organização estrutural de entidades de uma ICP, instalação, configuração e entendimento do modo de operação do SGCI, que é a base estrutural da sugestão proposta para ser implantada na UFSM, bem como a instalação e configuração do ambiente hospedeiro da ferramenta englobando, principalmente, o banco de dados e o servidor *web.*

Também foram realizadas pesquisas aprofundadas relativas à ferramenta AC-Correio, que, como afirmado anteriormente, já foi instalada e configurada para que testes pudessem ser realizados e conclusões pudessem ser obtidas. A AC-Correio é uma ferramenta que atua em conjunto com o SGCI e é de suma importância, visto que é através dela que será emitida a maior parte dos certificados, afinal a mesma atua como interface para que a comunidade acadêmica da UFSM possa requerer seus certificados.

Ao final deste estudo, para chegar à oferta efetiva do serviço de certificação digital ao usuários na UFSM, falta apenas a decisão por parte da RNP sobre a abertura de sua ICP a novas IESs. Este trabalho fornece de forma completa uma estrutura a ser seguida para a implantação efetiva de uma ICP na UFSM e sua ligação à ICP da RNP.00c

REFERÊNCIAS

Alecrim, E. **Assinatura digital e certificação digital**. InfoWester, 2005. Disponível em: <http://www.infowester.com/assincertdigital.php>. Acesso em: 20 out. 2007.

Carlos, M. C. **Topologias dinâmicas de infra-estruturas de chaves públicas.** Florianópolis: UFSC, 2007. Tese de Mestrado.

Custódio R. F. **GT - ICP-EDU:** Manual de Sistemas da Infra-estrutura de Chaves Públicas Educacional. RNP, 2005.

Custódio R. F.; Graaf J. V.; Dahab R. **GT - ICP-EDU:** Uma Infra-estrutura de Chaves Públicas para o Âmbito Acadêmico. RNP, 2003.

E-Bit. **Comércio eletrônico cresce 49% no primeiro semestre de 2007,** 2007. Disponível em: <http://www.ebitempresa.com.br/ebit_informa/html/indice_08_10_2007.asp>. Acesso em 05 out. 2007

E-SEC. **Princípios de assinatura digital**. Brasília, 2001. Disponível em: <www.digitrust.com.br/AssinaturaDigital.doc>. Acesso em: 20 out. 2007.

Ignaczac, L. **Um novo modelo de infra-estrutura de chaves públicas para uso no Brasil utilizando aplicativos com o código fonte aberto**. Florianópolis: UFSC, 2002. Tese de mestrado.

LabSEC. **Digital Certification Package**, 2006. Disponível em: <https://projetos.labsec.ufsc.br/pcd>. Acesso em: 21 out. 2007.

Lins, B. F. E. **Comércio eletrônico, assinatura e certificação digital.** Brasília: Consultoria Legislativa, 2005.

MICROSOFT. **Infra-estrutura de Chaves Públicas**. 2005. Disponível em: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/pt-pt/library/ServerHelp/32aacfe8-83af-4676-a45c-75483545a978.mspx?mfr=true>. Acesso em: 02 nov. 2007

Müller, E. M. **Estudo e implementação de autenticação no acesso para o portal do HUSM**. Santa Maria: UFSM, 2007. Trabalho de Graduação.

OpenBSD. **Introdução ao OpenBSD**, 2004. Disponível em: <http://www.openbsd.org/faq/pt/faq1.html>. Acesso em: 19 out. 2007.

PostgreSQLBR. **O que é o PostgreSQL?** 2006. Disponível em: <http://www.postgresql.org.br/Introdu%C3%A7%C3%A3o_e_hist%C3%B3rico>.

Acesso em: 15 dez. 2007.

RNP. **O *Hardware* do HSM RNP-Kryptus.** 2006a. Disponível em: <http://www.esr.rnp.br/leitura/index.php?categoria=3&arquivo=22>. Acesso em: 17 out. 2007.

RNP. **RNP lança autoridade certificadora raiz para a comunidade acadêmica**. 2006b. Disponível em: <http://www.rnp.br/noticias/2006/not-061207b.html>. Acesso em: 19 out. 2007.

RNP. **Certificação e TV digitais são temas do terceiro dia do SCI**. 2007. Disponível em: <http://www.rnp.br/noticias/2007/not-071025a.html>. Acesso em: 26 out. 2007.

Vigil, M. A. G. **Autoridade certificadora de correio eletrônico**. Florianópolis: UFSC, 2007. Trabalho de Graduação.

WNews. **Certificação Digital.** 2006. Disponível em: <http://wnews.uol.com.br/site/noticias/>. Acesso em: 19 out. 2007.

Zen, Eliana. **Produtividade no uso de Prontuário Eletrônico do Paciente na Unidade de Cardiologia do HUSM**. PPGEP-UFSM, Santa Maria, 2008. Dissertação de Mestrado.