Certificação Digital Acadêmica: Implantação do Sistema de Gerenciamento de Certificados Digitais ICPEDU na UFSM

Diego Mostardeiro Friedrich[1] - dmf@inf.ufsm.br
Roseclea Duarte Medina[1] - rose@inf.ufsm.br

[1] Curso de Ciência da Computação
Universidade Federal de Santa Maria (UFSM)

Resumo. *O Sistema de Gerenciamento de Certificados Digitais desenvolvido pelo grupo de trabalho ICPEDU é uma ferramenta que pode ser utilizada para criar e gerir Infra-estruturas de Chaves Públicas (ICP), permitindo o controle total de seus certificados digitais, assim como emissão, revogação e publicação. Entretanto, essa é uma nova ferramenta que possibilita uma alternativa diferenciada do uso de certificados digitais. Este trabalho realiza uma análise das características e do funcionamento dessa ferramenta, realçando seus pontos positivos e negativos e sua implantação na Universidade Federal de Santa Maria (UFSM), objetivando atender as necessidades de segurança nos projetos de educação a distância (EAD).*

Palavras-chave*: certificação digital acadêmica, infra-estruturas de chaves públicas, certificados digitais, educação a distância.*

Abstract. *The Management System Certificates Digital developed by the working group ICPEDU is a tool that can be used to create and manage a Public Key Infrastructure (PKI), allowing complete control of their digital certificates, as well as issuance, revocation and publication . However, this is a new tool that allows an alternative differentiated use of digital certificates. This work is a comprehensive analysis of the characteristics and the operation of this tool, highlighting their positive and negative points and their deployment at the Federal University of Santa Maria (UFSM), looking to find the needs of security in the projects of the distance education (TDE).*

Keywords: *Academic Digital certification**,** public key infrastructure, digital certificates, the distance education.*

1. Introdução

O cotidiano torna-se cada vez mais acostumado com a insegurança existente no dia-a-dia das cidades e do mundo como um todo. Por tais condições, os indivíduos passam a tomar medidas mais rígidas para que fatos desagradáveis não venham a lhes comprometer. No meio digital o mesmo comportamento vem tomando mais espaço a cada dia através de pesquisas, implementações e atitudes que tomam como premissa aumentar a segurança das informações compartilhadas através da Internet.

Neste meio, a segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização, formalizados nos termos de uma política de segurança. (Soares, Lemos, Colcher 2000 p448).

A certificação digital situa-se nesse contexto e surgiu para melhorar a segurança das informações que trafegam pela grande rede. Esse é um, entre tantos outros benefícios, que um certificado digital, se utilizado de forma correta, pode prover sobre as informações, pois, além de utilizar o artifício da criptografia, também armazena dados de seu proprietário a fim de garantir o não-repúdio de mensagens (Felippe, 2006).

A grande dedicação nessa área também é conseqüência da intensidade na qual vem crescendo a alternativa da substituição do papel por documentos eletrônicos seguros e, como citado acima, pela busca por segurança nas transações, já que o comércio eletrônico vem quebrando recordes de faturamento a cada ano que passa (IDG Now, 2007), assim como os cursos de educação a distância (EAD) que vêm surgindo não só em âmbito nacional como no mundo todo.

A Universidade Federal de Santa Maria (UFSM) não é exceção. Neste ano, a Instituição teve um crescimento meteórico de EAD, pois vinha oferecendo apenas um curso nesta modalidade e agora já oferece onze. Os quais são oferecidos através da utilização do ambiente virtual de aprendizagem Moodle integrado com o Sistema de Informações para o Ensino (SIE) da Instituição e também da integração dos sistemas de oito universidades que atuam em rede para oferecer seis cursos a distância na REGESD/PROLIC II[1]. Neste contexto criou-se um ambiente onde trafegam muitas informações sigilosas como históricos escolares e notas de provas, existindo a necessidade de um cuidado meticuloso com a segurança na transferência e armazenamento destas informações. No entanto, é claro o fato de que a Instituição de ensino Superior (IES) não ter condições de arcar com despesas de uma certificação digital comercial.

É nesse sentido que o Sistema de Gerenciamento de Certificados (SGCI), desenvolvido pelo grupo de trabalho Infra-estrutura de Chaves Públicas Educacional (ICPEDU), passa a ser uma ferramenta de grande valia, pois sua proposta prima pela segurança das informações e sem custos com licenças para utilização.

Desse modo, têm-se como objetivo neste artigo realizar uma explanação sobre o assunto, mais especificamente sobre o SGCI com o propósito de apresentar uma análise do funcionamento de tal ferramenta, assinalando suas principais características e sua implantação na UFSM.

2 Certificação Digital Acadêmica

2.1. 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. (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.

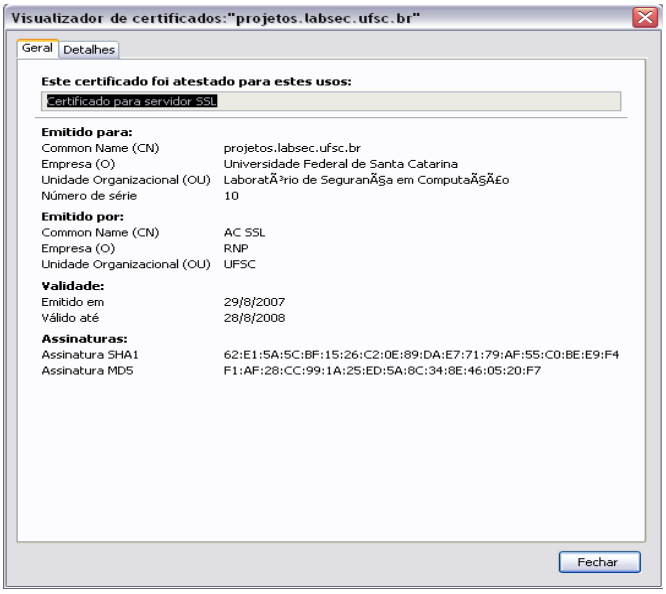

Figura 1 - Exemplo de Certificado Digital

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.

2.2 Certificação Digital Acadêmica

A partir das necessidades e também 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), uma das instituições de maior influência na área, 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 GT ICP-EDU, desenvolvido em cooperação entre algumas Universidades brasileiras, tais como a Universidade Federal de Minas Gerais (UFMG), a Universidade Federal de Santa Catarina (UFSC) e a Universidade Estadual de Campinas (Unicamp), e que possui como objetivo melhorar a segurança digital no âmbito acadêmico. Atualmente encontra-se em fase experimental pelas instituições que desenvolvem o sistema, sendo que em 2008 existe a previsão de abertura para outras IES (RNP, 2007).

Com base nos resultados obtidos por esse grupo de trabalho, que é o pioneiro no País, têm-se a possibilidade de implantação de uma ferramenta poderosa para a proteção da informação em sistemas e serviços que atuam na Internet atendendo aos mesmos requisitos da certificação digital nos moldes comerciais. 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.

Este é, entre outros pontos, um benefício o qual tal ferramenta proporciona. Contudo, nessa alternativa o funcionamento é totalmente de forma gratuita e eficiente para instituições de ensino e seus usuários para que, assim, os mesmos possam usufruir dessa nova tecnologia.

2.3 SGCI – Sistema de Gerenciamento de Certificados ICPEDU

No ano de 2001, a ICP Brasil foi reconhecida legalmente através da instituição da Medida Provisória nº 2.200-2 (Lins, 2005), antes disso, 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 algum tipo de segurança, pois não existia alguma ligação entre a chave enviada para o diretório e o usuário que a enviou (Ignaczac, 2002).

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.

2.3.1 Estrutura

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

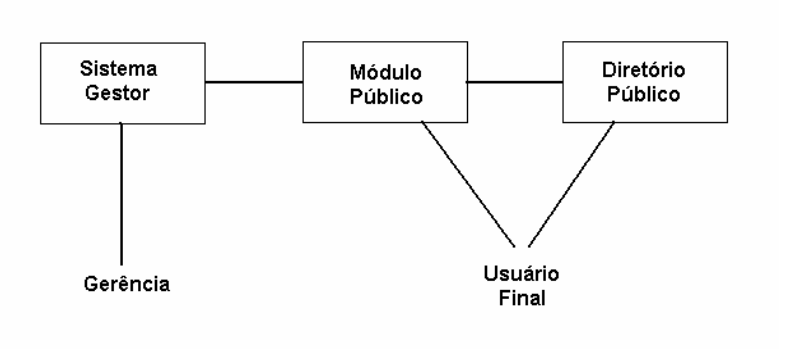

Figura 2 - Estrutura do SGCI

O sistema gestor engloba a criação e gerenciamento de Autoridades Certificadoras (AC's), que possuem basicamente as funções de criar e assinar certificados, publicar listas de certificados válidos e revogados mantendo informações sobre tais certificados e de Autoridades de Registro (AR's) que têm a finalidade de verificar a veracidade das informações apresentadas por alguém que esteja requisitando um certificado digital (Carlos, 2007).

O módulo público e o diretório público destinam-se aos usuários finais, pois o primeiro possibilita o fornecimento de certificados através de solicitação on-line, enquanto o outro consiste em um banco de dados de certificados válidos e uma lista de certificados revogados.

2.3.2 Módulo de Hardware Seguro

O grupo de trabalho eleito pela RNP desenvolveu o Módulo de Hardware Seguro ou Hardware Secure Module (HSM). Ele é um protótipo que, além de atuar como acelerador criptográfico, possui a finalidade de propiciar uma transmissão de dados realmente segura para sistemas de gerenciamento de certificados, para isso as universidades precisariam acoplar aos seus sistemas tal equipamento. 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.

Atualmente o sistema de gerenciamento de certificados acadêmico encontra-se em uso na UFSC e o desenvolvimento do HSM está em seu início de produção em maior escala, para que possa ser fornecido às instituições de ensino interessadas em tal dispositivo (RNP, 2007).

3. Certificação digital acadêmica – Projeto e implantação na UFSM

A RNP já possui inaugurada e em funcionamento sua AC-Raiz, que é a entidade de mais alto nível na hierarquia dessa ICP e a qual as instituições pertencentes ao ICPEDU atualmente são subordinadas, pois possuem seus respectivos HSM's, um dos quesitos primordiais para que seja efetivada tal subordinação. O objetivo seguinte da RNP é, a partir de 2008, abrir espaço para outras IES interessadas em fazer parte da ICP da RNP (RNP, 2006). 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 AC-Raiz ligada à RNP.

O trabalho, na UFSM encontra-se em fase inicial de 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 HSM's, 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. Encontra-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, é um dos grupos de pesquisa responsável pelo desenvolvimento do SGCI. A primeira opção nos direciona para uma estrutura uniforme, na qual instala-se todo o sistema a partir de um único pacote, chamado de Pacote de Certificação Digital (PCD) (LabSEC, 2006).

O PCD é um conjunto de programas contendo, além do sistema operacional, que é o OpenBSD, o próprio SGCI, 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 (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 nos leva a uma estrutura dividida em módulos, na qual o SCGI pode ser obtido separadamente 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. Existe a opção de instalação de dois outros módulos, 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.

Contudo, indiferentemente 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 bando de dados e servidor *web*.

Figura 3 - Tela inicial após a instalação do SGCI

Sua interface gráfica é amigável e seu uso é simples e fácil desde que os operadores possuam um conhecimento prévio do potencial da ferramenta no que diz respeito às funcionalidades, como por exemplo, os campos que dizem respeito ao período de validade do certificados, ao tamanho das chaves (quantidade de bits) geradas para o certificado, algoritmo a ser utilizado e usos permitidos ao certificado.

A organização dos operadores do sistema é feita através 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 AC's, AR's 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. Aos usuários finais cabe a solicitação de certificados e consultas sobre status de certificados no módulo público e diretório público respectivamente.

4. Considerações Finais

A certificação digital é uma assinatura virtual. Portanto, 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 sua conta corrente é você, evitando fraudes (WNews 2006).

Por essa importância e por todos 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. 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 em grandes economias com gastos em papel. O que, além de colaborar para a economia citada anteriormente, também ocasiona uma imensa diminuição do impacto ambiental.

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.

[1]REGESD/PROLIC II: Rede Gaúcha de Ensino Superior a Distância/ Programa Inicial para Professores dos Ensinos Fundamental e Médio II.

Referências

Alecrim, Emerson. **Assinatura digital e certificação digital**. InfoWester, 2005. Disponível em: http://www.infowester.com/assincertdigital.php. Acesso em: 20 de Outubro de 2007.

Carlos, M. C. **Topologias dinâmicas de infra-estruturas de chaves públicas.** Florianópolis: UFSC, 2007. 13p. Tese de Mestrado.

Felippe, Waldemar. **Certificação Digital - A validade e aplicabilidade do e-CNPJ na Assinatura Digital de Documentos Eletrônicos**, 2006. Disponível em: http://www.qualisoft.com.br/Artigos/Artigo200601-01.asp. Acesso em: 20 Outubro de 2007.

IDG Now. **Faturamento de lojas eletrônicas brasileiras cresce 49% no primeiro trimestre,** 2007. Disponível em: http://idgnow.uol.com.br/internet/2007/07/03/idg noticia.2007-07-03.1473966487/. Acesso em: 21 Outubro de 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 de Outubro de 2007.

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

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

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

Soares, L. F., Lemos, G., Colcher, S. **Redes de Computadores - das LANs, MANs e WANs às Redes ATM**. 2ª edição. Rio de Janeiro: Editora Campus, 2000.

WNews. **Certificação Digital.** Disponível em: http://wnews.uol.com.br/site/noticias/. Acesso em: 19 de Outubro de 2007.