Um Estudo sobre a Implantação e o Uso de Infra-Estrutura de Certificação Digital em Ambiente Universitário

Aluno: Eduardo Antonio Marchioro — **ra043079@fee.unicamp.br**

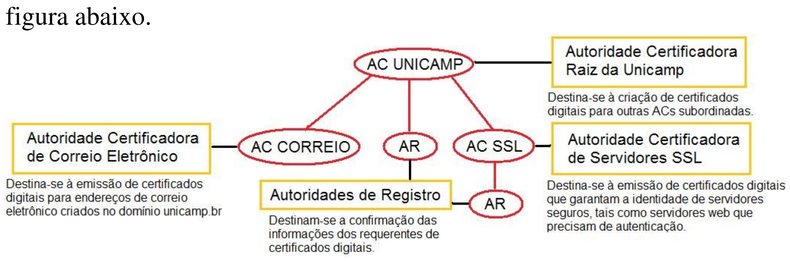
Orientador: Marco A. A. Henriques — **marco@dca.fee.unicamp.br**

Faculdade de Engenharia Elétrica e de Computação

Certificação Digital - Chaves Públicas - Criptografia

Introdução

O foco deste trabalho está em pesquisar e propor formas de implantar uma infra-estrutura de certificação digital para a comunidade acadêmica da Unicamp. Neste sentido foi necessária a criação de uma série de autoridades como pode ser observado na figura abaixo.



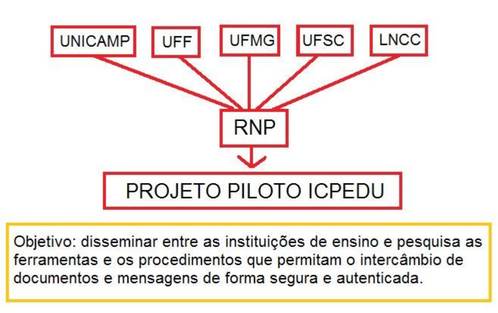
A assinatura digital de documentos é um recurso importante para a implantação futura de um sistema de Gestão Eletrônica de Documentos. No futuro, deseja-se implantar também uma AC-Pessoa, a qual deverá identificar eletronicamente um determinado indivíduo (e não apenas um endereço de e-mail). Para isso será necessária uma forte integração entre a ICP da Unicamp e os processos de emissão de identidade funcional e estudantil.

Metodologia

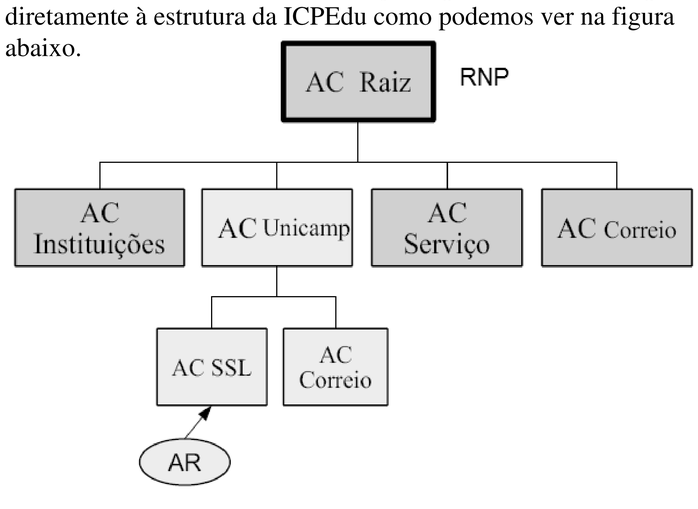
O método adotado para o desenvolvimento do trabalho incluiu a pesquisa e obtenção de material bibliográfico na internet, a participação em aulas sobre Segurança de Dados, a participação em apresentações, palestras e treinamentos promovidos pelo Grupo de Trabalho ICPEDU da RNP. Outro método foi o de preparação de um ambiente que permitisse testar e avaliar os programas implementados antes da sua utilização na AC Unicamp. Os módulos disponibilizados como software aberto pelo grupo de trabalho ICPEdu (Infra-estrutura de Chaves Públicas Educacional) da RNP/MCT foram usados como plataforma de testes para avaliar a implantação e alcançar as funcionalidades desejadas para a ICP da Unicamp.

Resultados e Discussões

A Unicamp, juntamente com outras universidades faz parte de um projeto de certificação digital em nível nacional conhecido como ICPEDU.

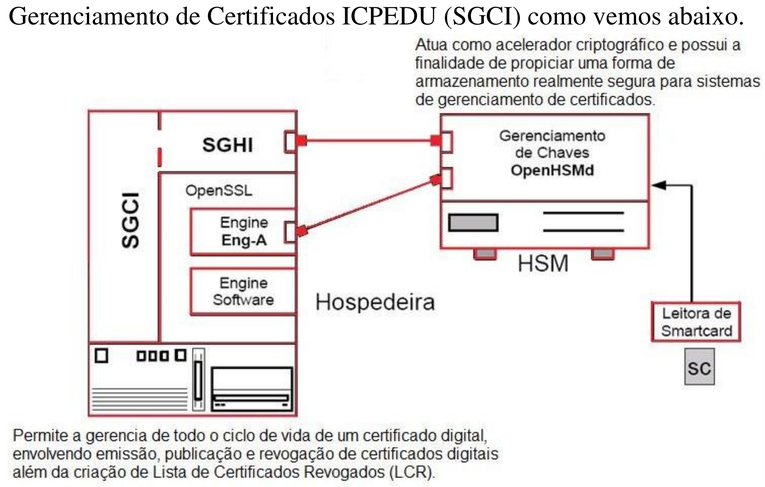


O principal resultado alcançado foi a criação de um piloto da infra-estrutura de certificação digital da Unicamp ligada diretamente à estrutura da ICPEdu como podemos ver na figura abaixo.

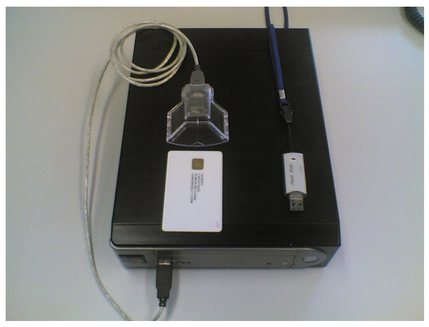


Resultados e Discussões

Para alcançar esse resultado, foram utilizados dois sistemas: uma máquina hospedeira com o OpenHSMd-Client-Java para a gestão do Hardware Secure Module (HSM) e o Sistema de Gerenciamento de Certificados ICPEDU (SGCI) como vemos abaixo.

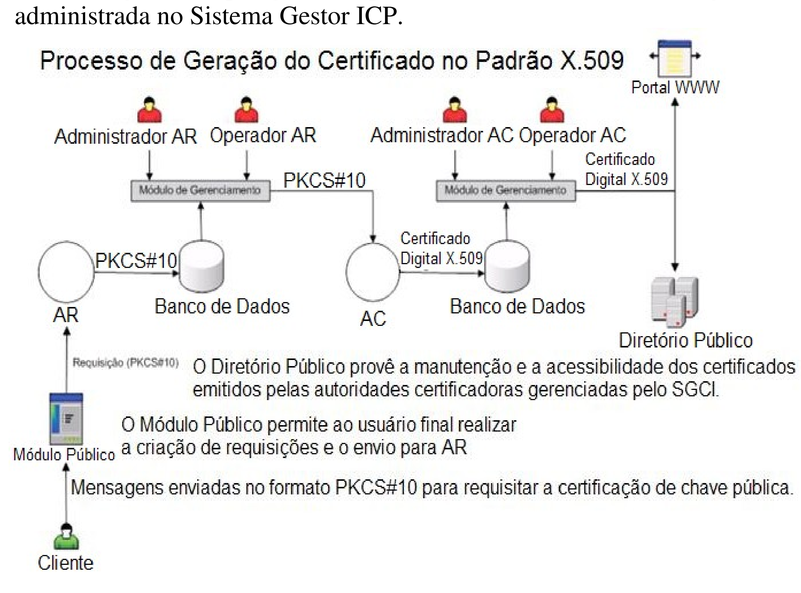


A partir da instalação do OpenHSMd-Client-Java foi possível conectar com o provedor de serviços criptográficos, que no caso, é o HSM. É através do HSM (figura ao lado) que iremos criar chaves criptográficas para serem usados nos certificados digitais na ICP da Unicamp.



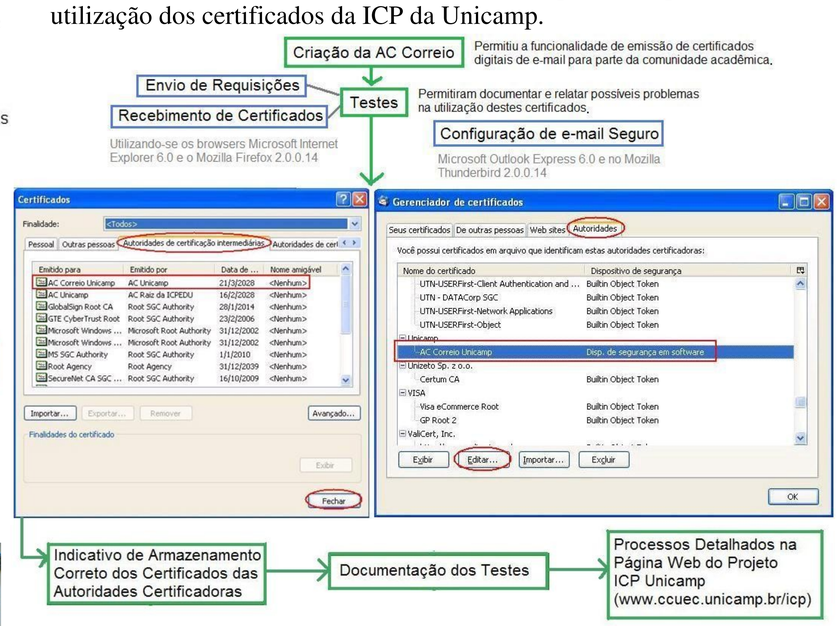
Outro resultado obtido foi a implantação do Sistema de Gerenciamento de Certificados ICPEDU (SGCI) que é um sistema dividido em três componentes funcionais básicos que são: o sistema gestor, o módulo público e o diretório público, como pode ser visto na figura abaixo.

Na figura abaixo podemos observar como é o processo de solicitação ou requisição feito pelo cliente e como essa solicitação é administrada no Sistema Gestor ICP.

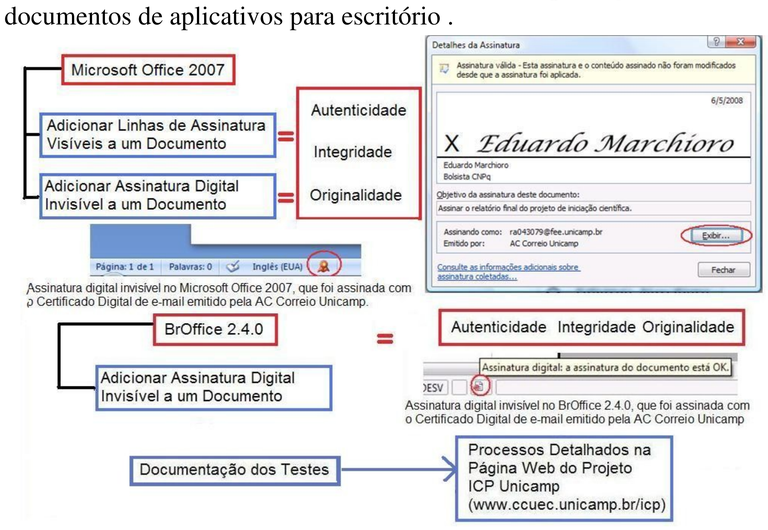


Resultados e Discussões

A partir da criação de uma AC Correio, iniciaram-se testes com o intuito de documentar e relatar possíveis problemas na utilização dos certificados da ICP da Unicamp.



Por fim, utilizou-se certificados digitais para assinar documentos de aplicativos para escritório .



Conclusão

Os principais objetivos do projeto foram alcançados. A criação de um ambiente de desenvolvimento e testes de aplicativos que interagissem com uma infra-estrutura de chaves públicas culminou nas cerimônias de criação da AC Unicamp e da AC Correio da Unicamp, como parte integrante do projeto desenvolvido pelo grupo de trabalho ICPEDU. Foi possível também a inauguração do primeiro serviço (AC Correio) disponibilizado ainda a uma parcela restrita da comunidade da Unicamp. Este serviço representa um avanço concreto numa área inovadora em se tratando de ambiente universitário, já que as infra-estruturas de chaves públicas disponíveis no país são pagas e inacessíveis a muitas pessoas. A ICPEDU é uma infra-estrutura que busca a diminuição dos custos de implantação dessa tecnologia e a formação de profissionais com conhecimento na área.

Referências

- Henriques, M. A. A., A Participação da Unicamp no Projeto Piloto de Infra-Estrutura de Chaves Públicas Educacional Brasileiro, Fórum Permanente de Conhecimento & Tecnologia da Informação: Documentos Digitais – Gestão e Legislação, CDC, Unicamp, jun/2007, http://www.cori.unicamp.br/foruns/tecno/evento22/marco_aurelio.pdf
- Martina, J. E., Vigil, M. A. G. V., Santos, E., Santos, D., Souza, T. C. S., Romani, J., Custódio, R. F., Manual do Usuário do OpenHSM, Laboratório de Segurança, Universidade Federal de Santa Catarina, http://www.icpedu.labsec.ufsc.br/tiki-download_file.php?fileId=241, dez/2005
- William Stallings, Cryptography and Network Security: Principles and Practice, Fourth Edition, Prentice-Hall, 2006