



XVI congresso interno de iniciação científica

Ginásio Multidisciplinar da Unicamp
24 a 25 de setembro de 2008



T1061

UM ESTUDO SOBRE A IMPLANTAÇÃO E O USO DE INFRAESTRUTURA DE CERTIFICAÇÃO DIGITAL EM AMBIENTE UNIVERSITÁRIO

Eduardo Antonio Marchioro (Bolsista PIBIC/CNPq) e Prof. Dr. Marco Aurélio Amaral Henriques (Orientador), Faculdade de Engenharia Elétrica e de Computação - FEEC, UNICAMP

O foco deste trabalho está em pesquisar e propor formas de implantar uma infra-estrutura de certificação digital para a comunidade acadêmica da 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 de um novo serviço como este. Neste sentido foi necessária a criação de uma Autoridade Certificadora Raiz (AC-Raiz) e sua correspondente Autoridade de Registro (AR). Esta AC-Raiz se destina à criação de certificados digitais para outras ACs subordinadas a ela como, por exemplo, AC-Correio e AC-SSL. A AC-Correio destina-se a emitir certificados digitais para endereços de correio eletrônico criados no domínio unicamp.br. Tais certificados permitem aos titulares das contas de e-mail enviar mensagens assinadas digitalmente ou criptografadas e, assim, a autenticidade e/ou a privacidade do remetente podem ser garantidos. A assinatura digital de documentos é um recurso importante para a implantação futura de um sistema de Gestão Eletrônica de Documentos. Já a AC-SSL tem por objetivo emitir certificados digitais que garantam a identidade de servidores seguros, tais como servidores web que precisam de autenticação. 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.

Certificação digital - Chaves públicas - Criptografia