INTEGRAÇÃO DE CARTÕES INTELIGENTES JAVA CARD A UMA INFRAESTRUTURA DE CHAVES PÚBLICAS PADRÃO USANDO SOFTWARE LIVRE

Aluno: Mauro Tardivo Filho
maurotfilho@gmail.com

Orientador: Prof. Marco Aurélio Amaral Henriques
marco@dca.fee.unicamp.br

Faculdade de Engenharia Elétrica e de Computação – FEEC/UNICAMP

Programa Institucional de Bolsas de Iniciação Científica – PIBIC/CNPq

Palavras-chaves: criptografia – chaves públicas – certificação digital

Introdução

Este trabalho pesquisou formas de integrar software livre na configuração e operação dos cartões inteligentes (smart cards) Java Card, utilizados como identidade funcional e estudantil na Unicamp, com a finalidade de integrá-los à Infraestrutura de Chaves Públicas de Ensino e Pesquisa (ICPEdu) implantada na universidade.

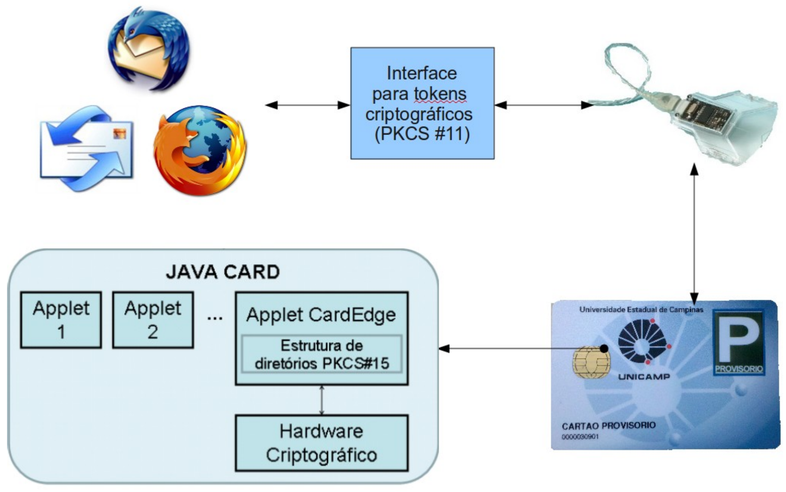

Figura 1: Camadas de software e hardware

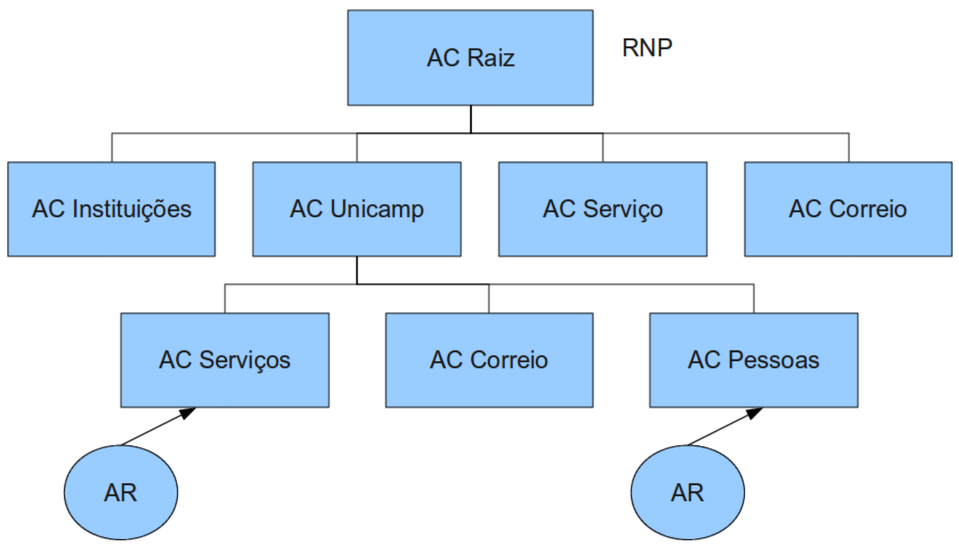

Figura 2: Infraestrutura de certificação digital da ICPEdu e da Unicamp

Resultados

Os seguintes resultados foram obtidos:

- aprendizado nos conceitos sobre segurança de dados
- aprendizado nos conceitos básicos sobre applets Java Card
- compilação e instalação no cartão de uma applet de segurança para armazenar chaves privadas e certificados
- configuração de um ambiente utilizando software livre para interagir com o cartão inteligente nos sistemas operacionais Microsoft Windows e GNU/Linux
- assinatura e cifragem de e-mails utilizando o Mozilla Thunderbird e o Microsoft Outlook
- assinatura de documentos utilizando a ferramenta BrySigner

Metodologia

A metodologia utilizada para este trabalho consistiu em pesquisa e obtenção de material bibliográfico na internet para aumentar o conhecimento sobre applets do cartão Java Card. Também foi possível, utilizando software livre, preparar um ambiente para compilar, configurar e utilizar a applet instalada no cartão em operações padrão de uma ICP.

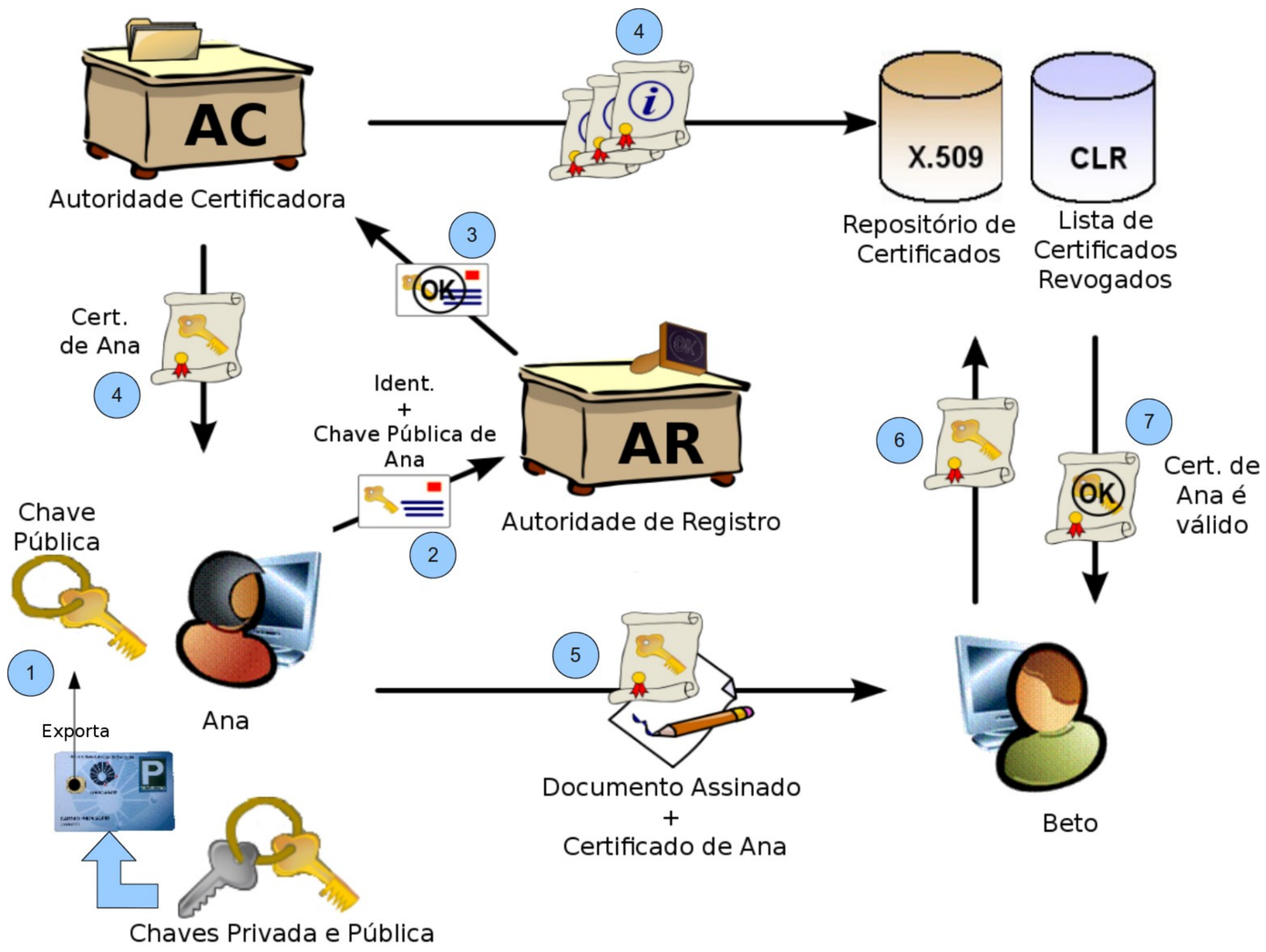

Figura 3: Infraestrutura de chaves públicas utilizando cartões inteligentes

Conclusões

Foi possível integrar o cartão inteligente usado na Unicamp a uma infraestrutura de chaves públicas padrão por meio da compilação e instalação no mesmo de uma applet específica para guarda de chaves e certificados. Isso permitirá à Unicamp prover maior segurança em processos de trabalho por meio de assinaturas digitais.

Referências Bibliográficas

[1] ICPEDU – Infraestrutura de Chaves Públicas de Ensino e Pesquisa, http://www.icp.edu.br/
[2] MUSCLE – Movement for the Use of Smart Cards in a Linux Environment, http://www.musclecard.com/
[3] OpenSC Project, http://www.opensc-project.org/