Proposta de mecanismos de assinatura digital e autenticação baseados no cartão universitário inteligente e na infraestrutura de chaves públicas de ensino e pesquisa ICPEDU

Aluno: Mateus José Figueiredo Lara
mlara@dca.fee.unicamp.br

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

Faculdade de Engenharia Elétrica e de Computação - **FEEC/UNICAMP**

Palavras-Chave: Assinatura Digital – Smart Card – Infraestrutura de chaves públicas

Programa Institucional de Bolsas de Iniciação em Desenvolvimento Tecnológico e Inovação (PIBITI) – Agência financiadora: **CNPq**

1. Introdução

Este trabalho buscou formas de se aproveitar os recursos criptográficos presentes no cartão universitário em uso na Unicamp e integrá-lo com uma infraestrutura de chaves públicas educacional, a fim de prover serviços de autenticação de usuários, de sigilo e de assinatura digital em documentos eletrônicos.

2. Conceitos Básicos

Figura 1: Geração de certificado

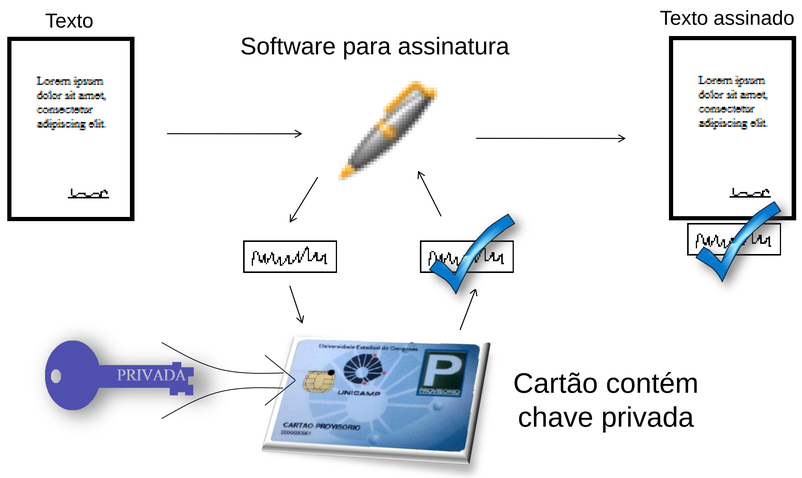

Figura 2: Assinatura de arquivo PDF

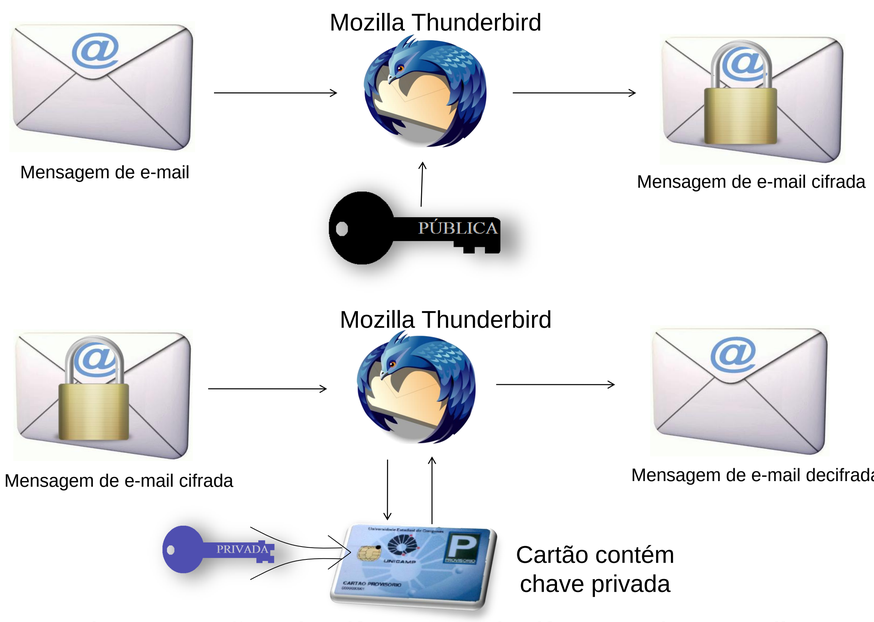

Figura 3a e 3b: Operações de cifragem e decifragem de e-mail, respectivamente

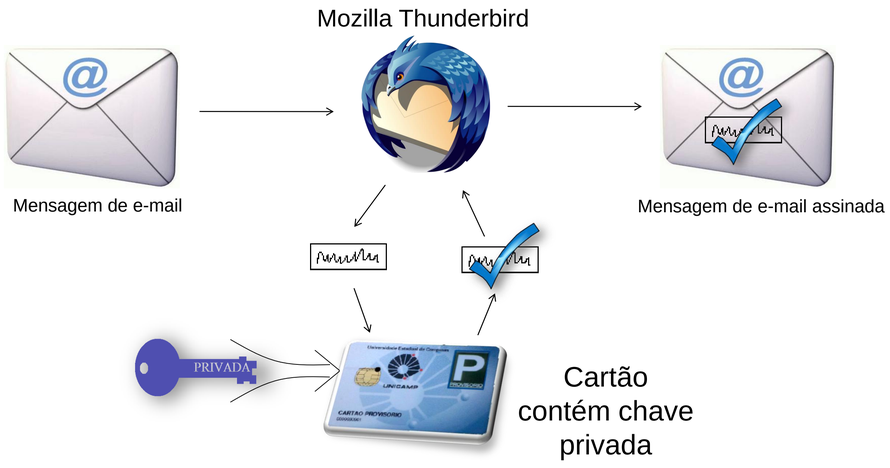

Figura 4: Assinatura de mensagens de correio eletrônico

3. Metodologia

Com os cartões Java Card e utilizando as *applets* do projeto M.U.S.C.L.E. (projeto que incentiva o uso de cartões inteligentes em ambientes Linux, mas também compatível com Windows) e Gemsafe (fabricante do cartão), buscou-se alternativas de software (principalmente software livre) que viabilizassem o uso do cartão inteligente para as operações de assinatura digital e autenticação. Foram utilizadas ferramentas da plataforma OpenSC (Open SmartCard), que possibilitam a integração de vários softwares com o cartão.

4. Resultados

Ao término do projeto, foi obtido um conhecimento mais profundo sobre os seguintes pontos:

- segurança de dados baseada em infraestrutura de chaves pública real;
- cartões inteligentes, incluindo as plataformas Java Card, OpenSC e M.U.S.C.L.E. ;
- configuração de ambientes Linux e Windows para interação com cartões inteligentes;
- geração de certificados nos cartões inteligentes com Autoridade Certificadora (AC) do projeto ICPEDU e com AC comercial (COMODO).
- cifragem e assinatura digital de mensagens de correio eletrônico (e-mail) cifradas e/ou assinadas digitalmente;
- geração e verificação de assinatura digital em arquivos PDF.

Este conhecimento foi detalhado em relatórios repassados ao Centro de Computação da Unicamp para que possa disponibilizar para a comunidade universitária mais serviços que usufruam da infraestrutura de chaves públicas que está sendo implantada.

A tabela a seguir sintetiza os principais resultados obtidos nas diferentes combinações de serviços, plataformas e ambientes operacionais. Um "NÃO" indica uma combinação que apresentou problemas funcionais, uma interrogação ("?") indica que os resultados não foram conclusivos, exigindo novos testes futuros e nos demais casos, está especificada com qual autoridade certificadora a combinação em questão foi bem sucedida, ICPEDU ou COMODO.

		Local de armazenamento da chave privada								
		M.U.S.C.L.E.			GemSafe			Disco rígido		
Geração de Certificados		ICPEDU/COMODO			ICPEDU/COMODO			ICPEDU/COMODO		
		Thunderbird	Outlook	Webmail	Thunderbird	Outlook	Webmail	Thunderbird	Outlook	Webmail
Correio Eletrônico	Assinar	COMODO	?	ICPEDU/ COMODO	COMODO	?	ICPEDU/ COMODO	COMODO	?	ICPEDU/ COMODO
	Verificar Assinatura	COMODO	?	NÃO	COMODO	?	NÃO	COMODO	?	NÃO
	Cifrar/ Decifrar	COMODO	?	ICPEDU/ COMODO	COMODO	?	ICPEDU/ COMODO	COMODO	?	ICPEDU/ COMODO
		DigiSigner	Libre Office	Adobe Reader	DigiSigner	Libre Office	Adobe Reader	DigiSigner	Libre Office	Adobe Reader
PDF	Assinar	NÃO	NÃO	ICPEDU/ COMODO	NÃO	ICPEDU/ COMODO	ICPEDU/ COMODO	NÃO	ICPEDU/ COMODO	ICPEDU/ COMODO
	Verificar Assinatura	ICPEDU/ COMODO	NÃO	ICPEDU/ COMODO	ICPEDU/ COMODO	NÃO	ICPEDU/ COMODO	ICPEDU/ COMODO	ICPEDU/ COMODO	ICPEDU/ COMODO
	Cifrar/ Decifrar	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	?	NÃO

5. Conclusões

Foi possível integrar o cartão inteligente universitário tanto à infraestrutura de chaves pública educacional como a uma comercial e assim realizar operações de cifragem, decifragem, assinatura e verificação com toda a segurança que o cartão pode oferecer para guarda de chaves privadas. Isto permitirá à comunidade da UNICAMP substituir assinaturas em papel por assinaturas digitais em documentos eletrônicos, minimizando o consumo de recursos e agilizando os trâmites internos. Ainda existem algumas situações em que o uso do cartão apresenta dificuldades e que precisam ser exploradas mais detalhadamente antes que os serviços correspondentes sejam disponibilizados à comunidade universitária.

6. Referências Bibliográficas

[1] ICPEDU – Infraestrutura de chaves públicas para ensino e pesquisa. http://www.icp.edu.br
[2] M.U.S.C.L.E. – Movement for the Use of Smart Cards in a Linux Environment. http://www.musclecard.com
[3] OpenSC Project. http://www.opensc-project.org