Desenvolvimento de ferramentas baseadas em software livre para integração de cartões inteligentes Java Card a uma infra-estrutura de chaves públicas

Aluna: Amanda Ortega de Castro Ayres – ra058767@fee.unicamp.br
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: Cartões Inteligentes - Segurança de Dados - Certificação Digital

Introdução

Smart card é um cartão que possui um chip com um microprocessador e uma memória embutidos, que podem ser usados com várias finalidades. O smart card usado como identidade funcional na Unicamp é mostrado na Figura 1.

Figura 1: Smart card usado na Unicamp

Criptografia é um mecanismo de segurança de dados que é usado para garantir que uma determinada informação não sofreu nenhuma espécie de ataque durante a transmissão entre duas partes. [1]

Existem dois tipos de algorítmos de criptografia utilizados: **criptografia simétrica** e **assimétrica**. Enquanto a criptografia simétrica utiliza a mesma chave para cifrar e decifrar a informação, a criptografia assimétrica utiliza um par de chaves diferente: uma **chave pública**, que é conhecida por todos, e uma **chave privada**, que deve ser guardada em sigilo pelo usuário.

Os algoritmos de criptografia assimétrica podem ser utilizados para **autenticação** (verificação da real identidade do remetente) e **sigilo** (certeza de que ninguém mais leu a mensagem). Para o sigilo, a chave pública é usada para cifrar mensagens, com isso apenas o dono da chave privada pode decifrá-la. Para autenticação, a chave privada é usada para cifrar mensagens, com isso garante-se que apenas o dono da chave privada poderia ter cifrado a mensagem, que pode ser decifrada por qualquer um com a chave pública. O esquema de funcionamento da autenticação de e-mails é mostrado na Figura 2.

Atualmente, os smart cards são equipados com um hardware criptográfico, o que torna possível sua utilização em operações criptográficas. O objetivo deste trabalho é integrar os smart cards usados na Unicamp, padrão Java Card, à Infraestrutura de Chaves Públicas Educacional (ICPEdu) em implantação na universidade. A vantagem de fazer essa integração é trazer mais segurança às operaçoes de cifragem e autenticação de mensagens, uma vez que a chave privada nunca sai de dentro do cartão e só pode ser usada por uma pessoa de posse do mesmo e que saiba uma senha de acesso.

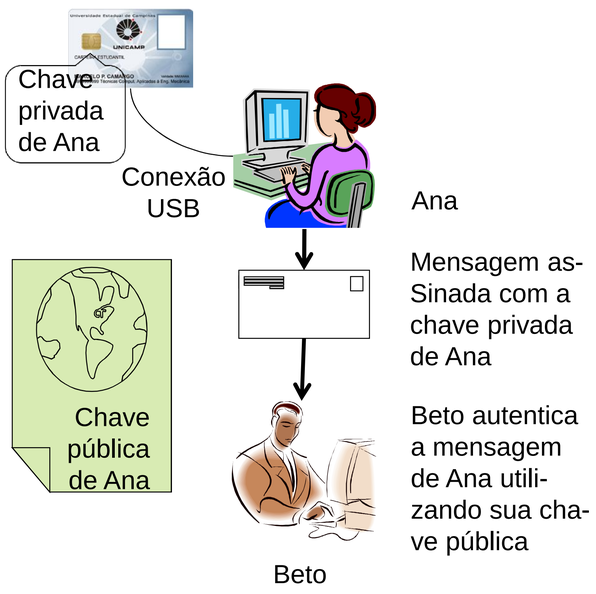

Figura 2: Esquema de autenticação de e-mail

Metodologia

A Figura 3 mostra as camadas de software e de hardware que foram utilizadas. Na camada número 1 encontram-se os programas que acessam o smart card a fim de realizar alguma operação criptográfica, como Thunderbird, OpenOffice e Firefox.

Na camada número 4 encontra-se o smart card padrão Java Card, composto por diversos programas, denominados applets, que funcionam de maneira independente uns dos outros.

Para que seja possível a utilização dos recursos criptográficos do cartão, foi instalada uma applet denominada CardEdge, que é fornecida por um projeto de código livre denominado MUSCLE [2].

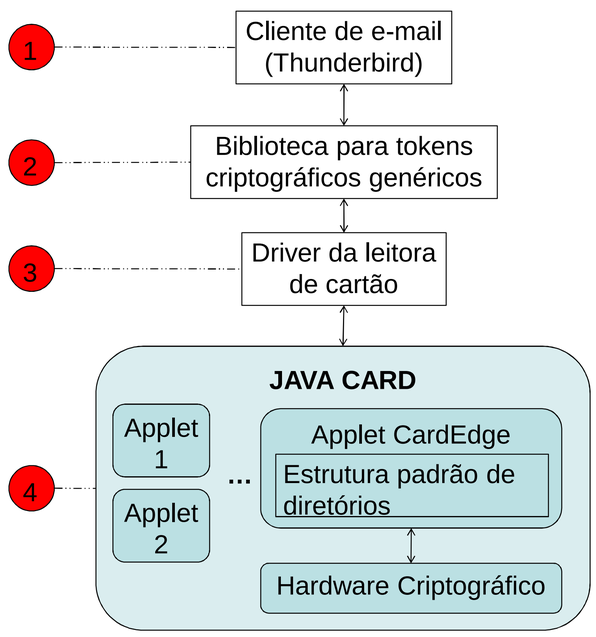

Figura 3: Camadas de software e hardware utilizadas

Para que fosse feita uma interação padrão entre os aplicativos e o cartão, foi implementada, através de um outro projeto chamado OpenSC [3], uma estrutura padrão de diretórios e arquivos junto à applet CardEdge.

Para fazer a integração entre as camadas 1 e 4, existem mais duas camadas de software: uma biblioteca que implementa uma interface genérica a tokens criptográficos (número 2) e o driver da leitora de smart card (número 3), que é específico de cada fabricante e é usado para o nível mais baixo de comunicação entre o computador e o cartão.

Resultados

Versões de teste do cartão foram integradas à Infraestrutura de Chaves Públicas em implantação na Unicamp. Os seguintes resultados foram obtidos:

✓ Assinatura e cifragem de e-mails utilizando o programa Thunderbird;

✓Assinatura de arquivos utilizando o programa OpenOffice.

As Figuras 6 e 7 mostram janelas do Thunderbird: na Figura 6 é exibido o certidicado que está armazenado no cartão e na Figura 7 é mostrada uma verificação do e-mail assinado utilizando o smart card.

Conclusões

Com a integração dos smart cards a Infraestrutura de Chaves Públicas torna-se possível o envio e recebimento de e-mails assinados e/ou cifrados utilizando o chip do cartão para gerar e armazenar o par de chaves.

Ainda não foi obtido êxito na operação de login utilizando o par de senhas do cartão para identificação do usuário.

Referências

✓ [1] Cryptography and Network Security, William *Stallings*

✓ [2] MUSCLE - Movement for the Use of Smart Cards in a Linux Environment, http://www.musclecard.com/

✓ [3] opensc-project.org - Home of open source smart card solutions, http://www.opensc-project.org/

Figura 5: Certificado existente dentro do cartão selecionado para assinar/cifrar e-mails.

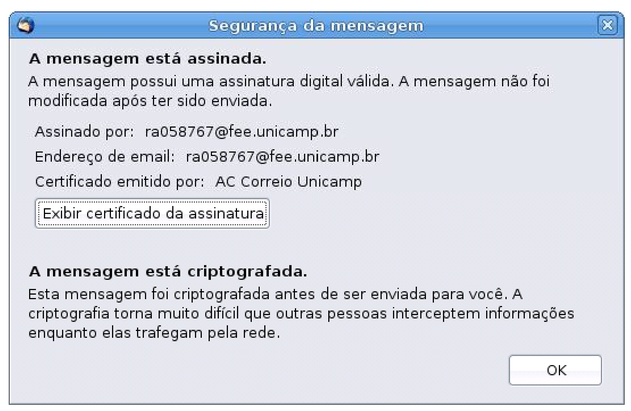

Figura 6: Janela de verificação do e-mail assinado e cifrado utilizando o smart card