CEFET CARD : CARTÃO INTELIGENTE PARA O SERVIDOR DO CEFET

Gleison Tavares DIOLINO (1); Fellipe Araújo ALEIXO (2); Leonardo Ataíde MINORA (3);
(1) CEFET-RN, Av. Sen. Salgado Filho, 1559, Tirol, Natal-RN – CEP: 59015-000, telefone: (84) 4005 2637, e-mail: gtdiolino@gmail.com
(2) CEFET-RN, e-mail:fellipe@cefetrn.br
(3) CEFET-RN, e-mail:minora@cefetrn.br

RESUMO

Com a evolução da tecnologia de microprocessadores, hoje é possível instalar um minúsculo chip em um cartão de plástico, nas dimensões de um cartão de crédito convencional. Chip este com capacidade de armazenamento de informação e processamento. Esse tipo de cartão é chamado de Smart Card. Podem ser desenvolvidas aplicações para esses cartões utilizando um subconjunto da plataforma Java, Java Card. As aplicações desenvolvidas, chamadas de *applets Java Card*, possuem as características de segurança, necessárias para uma vasta gama de aplicações. Os dados armazenados no cartão não podem ser acessados diretamente. Para instalar, remover e interagir com uma aplicação instalada no cartão inteligente é necessário solicitar a uma aplicação "gerente", chamada de *card manager*, realizando antes um processo de autenticação. O objetivo do trabalho é explorar o potencial da plataforma *Java Card*, desenvolvendo uma aplicação voltada a oferecer um conjunto de funcionalidades para um servidor do CEFET, tais como: controle de ponto, controle de acesso a ambientes, autenticação no sistema acadêmico, entre outras. A pesquisa é um estudo de caso do desenvolvimento da aplicação CEFET CARD. A realização do trabalho foi organizada nas seguintes atividades: (1) levantamento de requisitos, (2) modelagem das funcionalidades, (3) implementação e (4) testes.

Palavras-chave: *Smart Card*, *Java Card*, Cartão Inteligente, CEFET CARD.

1. INTRODUÇÃO

A evolução da indústria microeletrônica permitiu o surgimento dos *smart cards*, cartões de plástico que possuem um microprocessador e memória, tendo a capacidade de armazenar informações e processá-las. Devido a essas características, os *smart cards* são bastante seguros, já que os dados necessários estão guardados internamente e as transações podem ser executadas *offline*. Por isso, eles são geralmente utilizados para armazenamento seguro desses dados, autenticação e segurança de transações, já que também possuem a vantagem de os dados não poderem ser facilmente copiados ou utilizados por outra pessoa.

As principais aplicações dos *smart cards* são cartões de telefone pré-pagos, sistemas GSM (*Global Sisitem for Mobile Communication*), cartões de crédito ou débito seguros, tarifa de transporte coletivo, acesso a ambientes, dentre outras.

A tecnologia Java Card, desenvolvida pela Sun MicroSystems, surgiu para oferecer aos *smart cards* as mesmas vantagens da tecnologia Java: interoperabilidade, dinamicidade, suporte a múltiplas aplicações e segurança. Essa tecnologia é uma adaptação da plataforma Java, com várias restrições, mas que oferece um ambiente de execução compatível com as características dos *smart cards*: memória, comunicação e segurança.

1.1 JUSTIFICATIVA

Esse projeto visa à implementação de um sistema que oferece ao funcionário do CEFET-RN um cartão com as seguintes funcionalidades: registro de ponto, acesso a ambientes e autenticação ao sistema acadêmico. Esse cartão será um *smart card* com a tecnologia Java Card, já que ela oferece as características necessárias para a realização dessas operações. O proposto é que cada funcionário possua um cartão com suas informações pessoais armazenadas.

Toda instituição possui um sistema de registro de ponto de seus funcionários, seja este manual ou automatizado. No CEFET/RN, os funcionários possuem um crachá com um código de barras e é através da leitura desse código que eles se identificam. A proposta de substituir a identificação através de código de barras por *smart cards* se baseia nas vantagens que esses cartões apresentam na questão da segurança, uma vez que possuem poder de processamento e maior segurança no armazenamento de informações.
Outro aspecto existente na instituição é o acesso aos laboratórios e salas de aula. A permissão de acesso é garantida apenas por uma lista de pessoas autorizadas a pegar a chave de determinada sala. A solução proposta para um melhor controle e uma maior segurança é utilização de *smart cards, em* que as portas sejam automáticas e ligadas a um leitor, que se comunique com o cartão para que ele próprio verifique a permissão de acesso.
Outro problema identificado é o acesso ao sistema acadêmico. Como há uma diferença de permissões entre professores e gerentes, por exemplo, é necessário que seja feita uma diferenciação de quais modificações cada um pode fazer dentro do sistema. Tudo que é preciso para ter acesso ao sistema é digitar uma senha, o que passa a ser uma falha de segurança se essa senha for descoberta e utilizada por outra pessoa que não possua as mesmas permissões. A proposta é integrar esse sistema a um sistema de autenticação que utiliza *smart card*, garantindo maior segurança e veracidade no processo de autenticação do funcionário.

1.2 OBJETIVOS

Propor, documentar e implementar um sistema que ofereça maior controle e segurança às atividades realizadas pelos funcionários do CEFET-RN, através da utilização de *smart cards*, a fim de otimizar algumas de suas atividades na instituição.

1.3 METODOLOGIA

O primeiro passo foi estudar os conceitos relacionados a *smart cards* e compreender aspectos da tecnologia Java Card, para implementação de aplicações que são executadas dentro do cartão. Posteriormente, houve o aprofundamento de alguns conceitos da UML e o estudo do processo de desenvolvimento de *software* PAS (Processo Acadêmico Simplificado), utilizado para documentar o desenvolvimento do sistema. Toda a pesquisa foi realizada através de livros, artigos e *sites* da *WEB.*

2. SMART CARDS

Os *smart cards,* cartões inteligentes, são cartões de plástico semelhantes aos cartões de crédito convencionais, que armazenam e processam informações, possuindo um microprocessador que lhes proporciona poder de processamento embutido.

As principais aplicações dos *smart cards* são cartões de telefone pré-pagos, sistemas GSM (*Global Sisitem for Mobile Communication*), cartões de crédito ou débito seguros, tarifa de transporte coletivo e acesso a ambientes. O *smart card* é a ferramenta ideal para tais aplicações, pois proporciona diversos benefícios como: poder computacional embutido, praticidade, flexibilidade de uso e segurança. Um cartão inteligente é extremamente seguro, pois a obtenção de informações necessita da posse física do cartão e de um conhecimento profundo do seu *hardware* e s*oftware*.

Os *smart cards* são padronizados para a indústria pela ISO (*Internation Organization Standardization*) 7816 e suas sete partes, que definem características físicas, dimensões e localização de contatos, sinais eletrônicos e protocolos de transmissão, entre outros. Chen (CHEN, 2004) também cita as seguintes especificações para *smart cards:* GSM (*Global Sisitem for Mobile Communication*), EMV (Europay , MasterCard e Visa), *Open Platform, Open Card Framework e PC/SC, além do Java Card.*

2.1. COMUNICAÇÃO

O leitor, denominado CAD (*Card Acceptance Device*), é o dispositivo utilizado para fazer a comunicação entre o *smart card* e um computador, conectado a ele através de uma porta USB, paralela ou serial. Um CAD pode ser classificado como leitor ou terminal. Os terminais são computadores que possuem um leitor como um de seus componentes, como por exemplo, os dispositivos utilizados em lojas para pagamentos e transações com cartões de crédito (CHEN, 2004).

A comunicação com o cartão é sempre iniciada pelo leitor, ou seja, o cartão nunca envia dados sem um estímulo externo. Isso representa um verdadeiro relacionamento mestre-escravo, com o leitor sendo o mestre e o cartão sendo o escravo.

A comunicação realizada com o cartão é feita através do envio e recebimento de APDUs (*Application Protocol Data Units*), especificada na ISO 7816-4. O APDU é um protocolo de nível de aplicação que está entre o *smart card* e a aplicação *host*, aplicação que se comunica com o cartão e que pode estar em um computador ligado a um leitor ou em um terminal. Existem duas estruturas possíveis de APDU, o C*ommand APDU* e o *response APDU*, a primeira é utilizada pela aplicação *host* para enviar comandos ao cartão e a segunda é utilizada pelo cartão para mandar respostas de volta. Essa comunicação é *half-duplexed*, isto é, os dados podem tanto ser enviados da aplicação *host* para o *smart card* ou dele para ela, mas não ambos ao mesmo tempo. Um *smart card* fica sempre passivo, esperando por um *command* APDU da aplicação *host*. Ele então executa a instrução especificada no comando e responde para o *host* com um *response* APDU. Essa troca de *command* e *response* APDUs está ilustrada na figura 1.

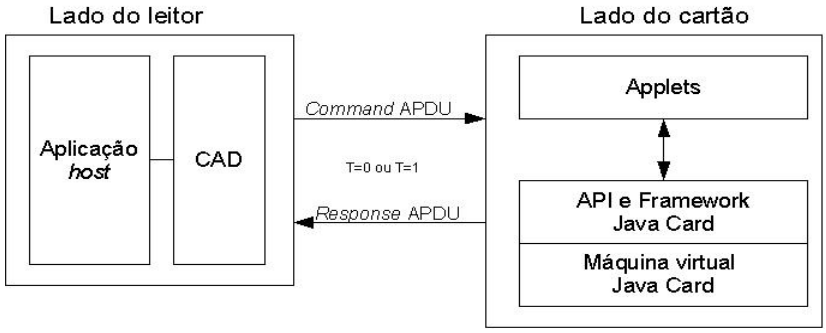

Figura 1 - Comunicação entre o host e o cartão (CHEN, 2004)

2.2. TECNOLOGIA JAVA CARD

A tecnologia *Java Card* é uma adaptação da plataforma Java para ser utilizada em *smart cards* e outros dispositivos cujos ambientes são altamente especializados, e cuja memória e restrições de processamento são mais severas do que as dos dispositivos J2ME[1] (MEIRELES e SOUZA, 2006). A tecnologia *Java Card* possui sua própria máquina virtual, API (*Application Programming Interface*) e especificação de *Run Time*, e está atualmente na versão 2.2.2.

2.3. APPLETS JAVA CARD E APLICAÇÃO HOST

Os *applets Java Card* são classes Java convencionais que estendem a classe javacard.framework.Applet, seguindo as especificações da tecnologia *Java Card*. (CHEN, 2004).

As classes e os *applets* são empacotados em um único arquivo denominado CAP (*Converted Applet*), conceito semelhante ao arquivo Jar. É esse arquivo que é instalado no cartão.

As aplicações *host*, aplicações externas ao cartão que se comunicam com ele, podem ser desenvolvidas em várias linguagens de programação. Para uma aplicação desenvolvida em Java, existe, dentre outras, a API nativa do Java chamada Smart Card I/O, que é um conjunto de bibliotecas que provêem a comunicação entre os *smart cards* e os *softwares hosts*.

3. PAS – PROCESSO ACADÊMICO SIMPLIFICADO

O Processo Acadêmico Simplificado (PAS), é um processo de desenvolvimento de software acadêmico, desenvolvido para ser aplicado no curso de Tecnologia em Análise e Desenvolvimento de Sistemas do CEFET/RN, nas disciplinas que envolvem a prática de desenvolvimento de software.

Ele é baseado no UP (*Unified Process*) e tem por objetivo ser mais simplificado, enxuto e adequado à realidade e às necessidades das disciplinas do curso que por ventura venham a fazer uso dele.

Busca, além de simplificar o processo e adequá-lo ao curso, trazer idéias e práticas de outros processos que possam enriquecê-lo (como valores e práticas do XP, ou mesmo métodos do ICONIX, etc.) e criar modelos de documentação específicos para ele.

Embora o processo seja baseado, essencialmente, no UP, são utilizados mais especificamente, três processos de desenvolvimento de software como orientadores na construção do PAS, quais sejam: RUP, ICONIX, XP.

---

1 J2ME (Java *2 Platform Micro Edition*) é uma edição da tecnologia Java para dispositivos móveis.

4. CEFET CARD

O CEFET Card é um sistema idealizado para oferecer ao funcionário do CEFET-RN uma melhoria na realização de algumas de suas atividades diárias. Essas melhorias estão tanto em questões práticas, como a automatização, como na questão da segurança das operações realizadas. Dentre os aspectos existentes na instituição, três deles foram inicialmente selecionados para implementação. A idéia é que cada funcionário possua um cartão (um *smart card* com a tecnologia Java Card) com suas informações pessoais armazenadas, através do qual ele possa registrar o ponto, requisitar acesso a ambientes (salas e laboratórios), além de manipular o sistema acadêmico de acordo com as restrições relacionadas à sua credencial.

O sistema possui dois níveis de operações, as que são realizadas pelo funcionário, utilizando seu cartão (registrar ponto, autenticar-se no sistema acadêmico, requisitar acesso a ambientes), e as que são realizadas pelo gerente para configurar o cartão (definição das informações pessoais como senha, matrícula, credencial e ambientes permitidos).

Resumidamente, o registro do ponto armazena em um banco de dados o horário que o funcionário entrou e saiu da instituição, a autorização de acesso a ambientes se dá de acordo com os ambientes permitidos ao funcionário, os quais estarão armazenados no cartão, e a autenticação no sistema acadêmico se baseia nas permissões de cada funcionário de acordo com sua credencial. Para que todas essas funcionalidades possam ser realizadas, é necessário que o usuário se autentique, digitando sua senha, cuja autenticidade é verificada pelo próprio cartão.

Em todas as operações, o funcionário interage diretamente com a aplicação *host*, cuja comunicação com o cartão é abstraída através da utilização da biblioteca “GP Comm”, definida em “GP Comm: Uma Biblioteca de Apoio à Comunicação com um Cartão Inteligente Compatível com a GlobalPlatform” (VIANA, 2007), não sendo assim necessária a manipulação direta de comandos APDU.

4.1. REGISTRO DO PONTO

O sistema atual de registro de ponto requer que o funcionário se identifique utilizando um crachá que possui um código de barras. A proposta de substituição desse sistema por um que utilize *smart cards* está baseada na questão da segurança, já que esses cartões são capazes de armazenar informações secretas de forma segura, devido ao seu suporte à criptografia, e processá-las, sem a necessidade de que essas informações saiam do cartão. O que garante a autenticidade do funcionário é o fato de ao inserir o cartão, ele ser identificado através da recuperação de sua matrícula, que se encontra internamente armazenada, e a requisição de sua senha, que é enviada ao cartão para que seja verificada, diminuindo bastante os problemas de fraude. A tela do sistema para o registro do ponto é exibida abaixo.

Figura 2 - Tela de Registro de Ponto

4.2 AUTENTICAÇÃO NO SISTEMA ACADÊMICO

A idéia de migrar o atual sistema de autenticação ao sistema acadêmico para um sistema que utilize *smart card* está fundamentada basicamente na questão da segurança. Isso ocorre devido à necessidade de diferenciação nas permissões de acesso relacionadas à credencial do funcionário. Isso significa dizer que existem operações que, por exemplo, podem ser realizadas apenas pelo gerente. Entretanto, no sistema atual, se uma senha for descoberta, uma pessoa que não deveria ter permissão pode passar a atuar no sistema acadêmico de forma perigosa. Para evitar esse tipo de problema, uma nova versão do sistema pediria que o funcionário inserisse seu cartão, para que não só a senha fosse verificada por ele, mas também para que o próprio cartão fornecesse a credencial daquele funcionário, garantindo assim uma maior segurança da transação.

Portanto, essa operação verifica a autenticidade do funcionário para que ele possa acessar o sistema acadêmico de forma mais segura, relacionando suas permissões no sistema com a credencial do funcionário, que pode ser: gerente, coordenador, secretário, professor ou funcionário.

4.3 AUTORIZAÇÃO DE ACESSO A AMBIENTES

A permissão de acesso aos laboratórios e salas de aula é garantida apenas por uma lista de pessoas que podem ter acesso. O controle é feito pela assinatura do funcionário e a informação do dia e hora em que a respectiva chave foi pega. O proposto é automatizar esse processo, garantindo maior segurança e controle, utilizando um *smart card* para armazenar e processar as informações necessárias. Para isso, as portas seriam automáticas, possuindo um leitor que só permitiria que a porta fosse aberta se o funcionário tivesse registrado o ponto e, conseqüentemente, ativado o cartão, além de ser verificado, pelo próprio cartão, se o funcionário possui direito de acesso aquele determinado ambiente e se a senha digitada corresponde à senha que está no cartão. O protótipo da tela do sistema para a operação de acesso a ambientes é ilustrada abaixo.

Figura 3 - Tela de "autorizar acesso a ambientes" - aplicação host

4.4 CONFIGURAÇÃO DO CARTÃO

Para que o cartão esteja apto a ser utilizado, primeiro é preciso configurá-lo. Essa configuração corresponde à instalação do *applet* e das outras classes necessárias no cartão, além da definição das informações pessoais de cada funcionário, como matrícula, senha, credencial e locais de acesso permitido, sendo possível também modificá-las após a primeira configuração, se necessário. A tela do sistema para configuração do cartão é ilustrada abaixo.

Figura 4 - Tela de configuração do cartão

5. CONSIDERAÇÕES FINAIS

5.1 CONCLUSÃO

O sistema resultante desse trabalho oferecerá um produto real como uma opção na melhoria de segurança e controle das atividades descritas. Ele se encontra em fase de construção.

O processo de desenvolvimento conta com o auxílio da biblioteca GP Comm, descrita em (VIANA, 2007) , utilizada para abstrair a complexidade existente na comunicação entre a aplicação *host* e um cartão inteligente. Outra ferramenta que auxilia no desenvolvimento desse projeto é o SMART INTERFACE (DIOLINO, ALEIXO, MINORA 2007), ferramenta que simplifica a interação com o cartão, encapsulando alguns processos mais complexos.

O processo de desenvolvimento de *softwares* PAS, utilizado para a modelagem do sistema descrito nesse trabalho, se encaixa bem por ser um processo relativamente pequeno e simples, sendo essa característica essencial devido à natureza complexa do sistema. A grande complexidade do sistema está ligada ao fato de envolver cartões inteligentes, pois cada caso de uso teve que ser analisado por dois ângulos: o da aplicação *host* e o do cartão, duplicando, assim, a quantidade de diagramas.

5.2 TRABALHOS FUTUROS

O sistema será concluído e poderá implantado a longo prazo, pois para sua implantação é necessário que sejam feitas algumas modificações em sistemas já existentes, além da aquisição e instalação de novos equipamentos.

Em relação ao registro de ponto, é necessário que a aplicação host desenvolvida interaja com o banco de dados já existente na instituição, para que possa recuperar os dados necessários e armazenar as informações do ponto. Quanto à funcionalidade de requisitar acesso a ambientes, se torna necessário a aquisição ou produção dos terminais para serem conectados às portas. Por fim, para a autenticação no sistema acadêmico é necessário que haja uma adaptação do sistema atual, o Q-Acadêmico, da Qualidata, para que este interaja com o cartão.

REFERÊNCIAS

CHEN, Zhiqun. **Java Card Technology for Smart Cards***:* Architecture and programmer´s Guid. San Antonio Road – California: Addison-Wesley, 2004. 368 p.

MEIRELES, Paulo. R. M.; SOUZA NETO, Plácido. A. **JML**: Design by Contract em Aplicações JavaCard. Natal-RN: Departamento de Informática e Matemática Aplicada (DIMAp) – Universidade Federal do Rio Grande do Norte (UFRN), 2006.

DIOLINO, Gleison T., ALEIXO, Fellipe A., MINORA, Leonardo A. **SMART INTERFACE**: FERRAMENTA DE AUXÍLIO AO DESENVOLVIMENTO DE APLICAÇÕES JAVA CARD. João Pessoa- PB: CONNEPI 2007.

VIANA, Crístian Dos Santos. **GP Comm**: Uma Biblioteca Java de Apoio à Comunicação com um Cartão Inteligente Compatível com a GlobalPlatform. Natal-RN: CEFET-RN, 2007. 106 p.

SUN MICROSYSTEMS. **Java Card Technology Overview**. Disponível em < http://java.sun.com/javacard/> Acesso em 2 de maio de 2008.