Uma proposta de emprego de s*mart cards* em infra-estrutura de chave pública

Rafael C. Figueiredo[1], Vinícius Gadis Ribeiro[1]

[1]Ciência da Computação – Centro Universitário La Salle (UNILASALLE)
Av. Victor Barreto, 2288 – 92010-000 – Canoas – RS – Brasil

rc_figueiredo@hotmail.com, vribeiro@unilasalle.tche.br

Abstract. *This paper approaches the use of the smart card technology as a way to intensify the public-key infrastructure, providing a safe way to protect cryptographic keys and digital certificates, besides offering security services of simple form and with mobility. Due to it, an open model for smart cards application in PKI was developed, in which services of authentication and digital signature are offered, both essentials for the infrastructure.*

Resumo. *O presente artigo aborda a utilização da tecnologia smart card como uma forma de intensificar a infra-estrutura de chave pública, provendo um meio seguro de proteger chaves criptográficas e certificados digitais, além de oferecer serviços de segurança de forma simples e com mobilidade. Em vista disto, foi desenvolvido um modelo aberto para aplicação de smart cards em PKI, onde são oferecidos os serviços de autenticação e assinatura digital, ambos essenciais para a infra-estrutura.*

Palavras chave: Segurança, Smart cards, PKI, Certificação Digital e Criptografia.

1. Introdução

Devido a crescente utilização da Internet e das redes privadas de comunicação, a quantidade de transações eletrônicas entre empresas e indivíduos aumenta a cada dia. Neste contexto, onde a circulação de grande volume de dinheiro e informações sigilosas é uma constante, surgiu naturalmente a necessidade de se ter garantias de segurança nessas transações [Hamann et al. 2001]. Assim como multiplicam-se o número de indivíduos e empresas que realizam transações eletrônicas, aumentam o número de pessoas com intenção de "prejudicar" estas transações de alguma forma. Para suprir esta necessidade, os sistemas baseados em criptografia de chave pública são largamente utilizados para garantir determinados fatores de segurança, identificando e autenticando pessoas e dispositivos [Burnett e Paine 2002]. Baseada neste modelo de criptografia, a tecnologia de PKI (*Public-Key Infrastructure* - Infra-Estrutura de Chave Pública) surgiu com o objetivo de resolver os problemas relacionados com a distribuição e certificação de chaves públicas, assegurando assim, que as comunicações eletrônicas sejam realizadas de forma segura para todos os envolvidos no processo.

A tecnologia PKI é baseada na utilização de certificados digitais, ou certificados de chave pública. Estes certificados têm como finalidade assegurar a confiabilidade e a procedência de uma chave pública. Para que toda a infra-estrutura funcione com a segurança que se é esperada, é necessário que se tenham determinados cuidados básicos, porém essenciais, na implementação e gerenciamento da PKI. Um ponto essencial e crítico da infra-estrutura é a garantira de segurança das chaves privadas nas entidades finais.

A criptografia de chave pública e o funcionamento dos certificados digitais dependem fortemente da segurança das chaves privadas. Isto significa que o indivíduo identificado no certificado deve manter em sigilo total a sua chave privada, e esta é uma das grandes dificuldades do processo. Como armazenar os certificados e as chaves privadas de forma segura no cliente? Como mantê-las e recuperá-las sem expor essas informações a situações de risco? Os *Smart Cards* (SC) são dispositivos que podem ser utilizados para resolver estas e outras deficiências de segurança.

Este trabalho propõem a utilização da tecnologia *smart card* para intensificar a infra-estrutura de chave pública, provendo um meio seguro de proteger chaves e certificados, além de oferecer serviços de segurança de forma simples e com mobilidade. Em vista disto, é apresentado um modelo de aplicação de *smart cards* em PKI, onde são oferecidos os serviços de autenticação e assinatura digital, ambos essenciais na infra-estrutura.

A relevância deste assunto afeta indiretamente todas as transações eletrônicas que exigem confidencialidade, integridade, autenticidade e não-repúdio. E é especialmente interessante às organizações que desejam implementar uma PKI utilizando algum tipo de *token* de autenticação. Entenda-se por *token*, todo dispositivo de hardware portátil que forneça um meio para identificar e autenticar um indivíduo [Burnett e Paine 2002].

O presente artigo está estruturado da seguinte forma: as seções 2 e 3 descrevem alguns conceitos sobre PKI e *smart cards*, respectivamente; a seção 4 apresenta os objetivos do modelo proposto, a metodologia utilizada no desenvolvimento e um exemplo de um cenário para a possível aplicação deste modelo; a seção 5 apresenta a análise e o projeto do modelo; e por fim, a seção 6 encerra com as conclusões e considerações finais sobre os estudos realizados.

2. Infra-estrutura de Chave Pública e Certificação Digital

PKI é uma infra-estrutura hierárquica baseada em confiança, que utiliza como elemento base uma estrutura de dados chamada de Certificado de Chave Pública (ou Certificado Digital), que tem como finalidade garantir a confiabilidade e a procedência de uma chave pública. Pode-se resumir uma PKI como sendo um conjunto de políticas de segurança, tecnologias de criptografia e protocolos de gerenciamento de chaves e certificados digitais [Mehdizadeh 2004].

Seja o seguinte cenário: Alice e Bob querem se comunicar de forma segura utilizando a tecnologia de chave pública. Para isto, Alice deve enviar sua chave pública para Bob, ou deixar a mesma em um local público onde Bob possa ter acesso, por exemplo, um servidor de uma rede local. Da mesma forma, Bob deve disponibilizar a sua chave pública para Alice. Quando Alice obtiver a chave de Bob, como ela terá certeza de esta chave realmente pertence ele? É possível que no intervalo de tempo entre Bob gravar a chave e Alice obtê-la, Mallory tenha acessado o servidor e trocado maliciosamente sua chave pública pela de Bob. Alice não terá um meio confiável de verificar a procedência da chave e assumirá que a mesma é de Bob. Então Mallory poderá interceptar a mensagem e lê-la sem nenhuma dificuldade, uma vez que somente a sua chave privada é capaz de descriptografa-la. Bob por sua vez, receberá a mensagem de Alice e não conseguirá lê-la, pois a chave pública utilizada para criptografar a mensagem foi a de Mallory, e não a sua.

Os Certificados de Chave Pública resolvem este problema, pois atestam a relação entre um indivíduo e sua respectiva chave pública como válida e confiável. Esta relação é fornecida por um terceiro publicamente confiável, isto é, uma entidade idônea a qual todos os envolvidos tenham como digna de confiança. Esta entidade, conhecida como Autoridade Certificadora (AC), é o único elemento em uma PKI responsável por emitir certificados e também é a única com poder de revogá-los, quando estes não forem mais válidos [Kiran, Lareau e Lloyd 2002].

2.1. Componentes de uma PKI

A definição da arquitetura de PKI foi publicada pelo IETF (*Internet Engineering Task Force*), através da recomendação ITU-T X.509, desenvolvida pelo grupo PKIX (*Public Key Infrastructure X.509*). A RFC3280 (*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*) descreve um modelo onde são definidos os componentes de uma PKI, bem como os relacionamentos entre eles.

A Autoridade Certificadora é a "fonte de confiança" de uma PKI, ela é a única entidade com poder de emitir e revogar os certificados de chave pública (assinados digitalmente antes de serem distribuídos). Os serviços mais comumente prestados por uma AC são: emissão de certificados de chave pública, emissão de CRLs (*Certificate Revocation List* - Lista de Revogação de Certificado), elaboração de políticas de segurança e certificação, *backup* e recuperação de chaves [Kiran, Lareau e Lloyd 2002].

Devido ao crescimento natural da infra-estrutura, a AC normalmente delega atribuições a outras entidades do sistema. Por exemplo, o serviço de registro de novos usuários é delegado a uma Autoridade Registradora (AR).

Uma Autoridade Registradora é basicamente um intermediário entre as entidades finais e a AC, realizando a prestação de diversos serviços, de forma a minimizar o trabalho desta. As funções de uma AR são: registrar os novos usuários de acordo com as políticas da AC, gerar chaves para as entidades finais, verificar e autorizar pedidos de revogação de certificados, backup e recuperação de chaves e publicação de CRLs [Burnett e Paine 2002].

As Entidades Finais são freqüentemente consideradas como usuários finais, mas seu conceito é muito mais abrangente. Uma entidade final pode ser uma pessoa física ou jurídica, hardware (como um roteador, *switch*, servidor, etc) ou software. Dependendo do ponto de vista, um provedor de serviços de PKI também pode ser considerado uma entidade final, por exemplo, uma AR é uma entidade final para um AC, da mesma forma que esta AC pode ser uma entidade final do ponto de vista da AC raiz [Kiran, Lareau e Lloyd 2002].

Para obter um certificado digital e tornar-se um membro da infra-estrutura, uma entidade final precisa ser registrada na PKI de acordo com as políticas de certificação da AC. Como já foi visto, este processo normalmente é realizado através da intermediação de uma AR, e dependendo do caso, pode exigir a presença física do cliente para que seja realizado o referido registro.

Outro componente importante da infra-estrutura são os chamados repositórios. Em uma PKI, um repositório é um local centralizado utilizado para armazenar informações pertinentes a infra-estrutura, como certificados e CRLs. Como exemplo de um repositório pode-se citar os diretórios de certificado e os servidores de *backup* e recuperação de chaves.

Pode-se citar também, um componente chamado de Emissor de CRL. Esta entidade é opcional na infra-estrutura, e é relativamente nova se comparada aos outros componentes (por isso não é comumente utilizada), sendo oficialmente padronizada no último modelo publicado pelo PKIX. Como o próprio nome diz, a função de um Emissor de CRL, nada mais é do que publicar e disseminar as Listas de Revogação de Certificados [Kiran, Lareau e Lloyd 2002].

2.2. Utilizando a Infra-estrutura

Diferentemente das chaves privadas, os certificados de chave pública não precisam ficar armazenados em um local necessariamente seguro, pois a informação que carregam é, teoricamente, de domínio público, e pode ser verificada por qualquer um que possua a chave pública da AC que

emitiu o referido certificado. Por outro lado, as chaves privadas necessitam de toda a segurança possível, e são mantidas de forma criptografada no cliente.

Considere o caso de um executivo que trabalha em uma empresa que utiliza uma infra-estrutura de chave pública. Ele possui um certificado digital e utiliza diversos programas da empresa onde é necessário utilizar sua chave privada para assinar documentos, como e-mails, contratos eletrônicos, e autorizações de compra de materiais. Quando os documentos assinados são enviados para terceiros, o certificado digital é enviado juntamente com o documento, de forma que o destinatário, mesmo sem ter acesso direto aos repositórios da PKI, consiga autenticar e verificar a integridade dos dados recebidos. Imagine que este executivo possui um *notebook*, o qual ele utiliza em viagens para realizar negócios a distância. Este usuário possui também um palmtop, que é usado quando ele está em movimento dentro da parque industrial da própria empresa, de forma a agilizar as autorizações de compras, e a resposta de mensagens importantes. Além disso, quando encontra-se em casa, ele utiliza seu PC (*Personal Computer*) para se conectar a VPN da empresa, para resolver eventuais problemas que venham a acontecer fora do horário de expediente ou em fins de semana.

Para que o usuário do caso a cima possa utilizar a PKI da empresa, será necessário que cada uma de suas máquinas (o PC da empresa e de sua casa, o *notebook*, e o *palmtop*) possua uma cópia de sua chave privada e de seu certificado digital. Obviamente esta não é um boa opção, pois estaria aumentando muito o risco de exposição da chave privada do usuário, além da série de problemas relacionados a manutenção de todas essas cópias.

A solução mais lógica para este problema é a utilização de um token seguro para permitir a mobilidade de chaves e certificados. Estes dispositivos superam com muitas vantagens os tradicionais métodos de armazenamento de chaves, pois possuem fortes características de segurança, além de promoverem a união entre a segurança física e lógica [Mehdizadeh 2004].

Na próxima seção será apresentada a tecnologia *smart card*, suas características, vantagens e desvantagens, e como ela contribui para aumentar o nível de alguns fatores de segurança em uma infra-estrutura de chave pública.

3. *Smart Cards*

Um *Smart Card* é um cartão composto de material plástico, padrão ISO (*International Organization for Standardization*), aparentemente igual a um cartão de crédito comum, mas que se diferencia por possuir um circuito eletrônico de silício integrado ao plástico.

Quanto a capacidade de processamento, os *smart cards* se dividem em dois tipos: cartões de memória e cartões "inteligentes" ou micro-controlados. Os cartões de memórias não possuem capacidades de processamento, e são utilizados apenas como um meio de armazenamento de dados. Apesar disso, esse tipo de cartão possui uma arquitetura de segurança lógica para acesso a memória. Os cartões chamados "inteligentes" possuem um microchip integrado que os permite realizar operações de leitura, gravação, cálculos matemáticos, além de carregar e executar programas internamente. Para aumentar o desempenho e o poder de processamento, muitos cartões possuem um co-processador criptográfico utilizado para realizar diversas operações criptográficas como DES, AES, RSA, SHA-1 entre outras [Burnett e Paine 2002]

Os *smart cards* também são classificados de acordo como a forma como comunicam-se com um terminal: com contato ou sem contato. Os cartões de contato exigem um contato físico do microchip com o terminal, de forma que este último ofereça energia para o cartão e o meio comunicação entre os dispositivos. Os cartões sem contato comunicam-se com o terminal através de radiofreqüência, eliminando a necessidade de contato físico entre as partes. Estes dispositivos

possuem uma antena de rádio (conectada ao *chip*) que se localiza entre o plástico do cartão, percorrendo toda a extensão da borda. Toda a comunicação entre um cartão sem contato e o terminal, é realizada de forma encriptada, para evitar que uma entidade estranha que esteja interceptando o sinal, tenha acesso aos pacotes de dados. Pode-se citar ainda um terceiro tipo de cartão que utiliza uma combinação dos dois tipos citados a cima, chamado cartão de interface dual ou combicard. Esse dispositivo pode comunicar-se por contato direto com o terminal ou através de radiofreqüência [Dreifus e Monk 1998].

3.1. Características de Segurança

A utilização correta da tecnologia SC (*Smart Card*) proporciona um duplo fator de autenticação e promove a convergência entre a segurança física e lógica, acarretando benefícios significantes para as organizações [Mehdizadeh 2004]. Processos de autenticação que utilizam SC exigem que o usuário esteja portando o cartão (fator de posse, algo que a pessoa tem) e saiba o seu código de acesso (fator de conhecimento, algo que somente a pessoa sabe). Essas duas exigências formam o duplo fator de autenticação que intensificam a segurança em sistemas que utilizam em *smart cards* [Longo e Stapleton 2002].

A utilização de uma tecnologia biométrica combinada com *smart cards* pode acrescentar um terceiro fator de autenticação ao sistema, o fator biométrico. Por exemplo, pode-se utilizar um SC para armazenar a impressão digital de um indivíduo, e no momento da autenticação comparar a impressão escaneada com a armazenada no cartão de forma a verificar se o portador é realmente o dono do cartão [Schneier 1996].

Smart cards tem a capacidade de isolar completamente do mundo externo os dados que armazenam em seu sistema de arquivos. Estes dados só podem ser recuperados através de uma comunicação entre o microchip e os programas que residem na memória do cartão, de forma que nenhuma informação pode ser lida ou gravada se os programas residentes não permitirem. Esta característica torna o *smart card* um dispositivo adequado para armazenar informações confidenciais como chaves privadas e senhas.

Outra importante característica de segurança são os cartões com co-processadores criptográficos capazes de processar algoritmos como DES, RSA, AES e curvas elípticas. Esta característica permite que sejam geradas assinaturas digitais, geração de chaves assimétricas, cifragem e decifragem de blocos dentro do cartão.

3.2. Normas e Padrões

A principal norma de padronização para *smart cards* é a ISO/IEC 7816, que possui atualmente dez partes, e define desde as características físicas dos cartões (largura, espessura, localização do *chip*, etc) até o protocolo de comunicação APDU e os dados que devem estar contidos no cartão para possibilitar a interoperabilidade entre indústrias. As normas ISO/IEC não utilizam o termo *smart card*, mas sim um termo mais genérico e correto: Cartão de Circuito Integrado (*Integrated Circuit Card* - ICC).

Baseadas nas normas ISO, surgiram iniciativas de diversas instituições com o objetivo de promover a tecnologia, padronizar e facilitar sua aplicação nos mais diversos fins e em diferentes plataformas. Um exemplo é o grupo EMV, formado pelo consórcio das empresas Europay, Mastercard e Visa, que tem como objetivo manter um padrão global para pagamentos eletrônicos utilizando *smart cards*.

Um dos grupos mais importantes atualmente é o GlobalPlataform que tem como missão estabelecer e manter padrões para uma infra-estrutura aberta de *smart card*, que possibilite aos provedores de serviços de diversas indústrias, desenvolver e manter aplicações compatíveis com a maior variedade de dispositivos existentes no mercado. Pode-se citar ainda o *OpenCard* (Framework para desenvolvimento de aplicações para *smart cards* baseado em Java), o PC/SC (*Personal Computer/Smart Card*) que visa a padronização entre computadores PC e leitoras de SC. Para a plataforma Linux destaca-se o MUSCLE (*Movement for the Use of Smart Cards in a Linux Environment*).

Dois sistemas operacionais estão consolidados no mercado atualmente, o JavaCard e o MULTOS (*MULTi-application Operating System*). Ambos possuem a característica de serem baseados em máquinas virtuais e terem a capacidade de gerenciar multi-aplicações, incluindo a funcionalidade de carga de novas aplicações após o cartão ter sido emitido e personalizado [DatacardGroup 2001].

JavaCard é um subset da linguagem Java, com uma menor quantidade de classes e uma série de limitações devido a capacidade de processamento dos *smart cards*. Em verdade, JavaCard não é um sistema operacional propriamente dito, mas sim uma série de especificações que definem como a máquina virtual JavaCard irá executar nos sistemas operacionais proprietários de cada fabricante. A versão atual do JavaCard é a 2.2.1, liberada pela Sun Microsystems em Outubro de 2003.

MULTOS é um sistema operacional aberto controlado pelo consórcio MAOSCO, da qual fazem parte empresas multinacionais com Axalto (divisão de *smart cards* da Schlumberger Limited), Hitachi, Infineon Technologies, Mastercard International, entre outras. O diferencial deste sistema operacional é a segurança, pois MULTOS é um dos poucos produtos não militares do mundo que possuem a certificação ITSEC nível 6 [DatacardGroup 2001].

3.3. *Smart Cards* e PKI

Há muitas vantagens em se implementar o uso de *smart cards* em uma PKI, em contrapartida verificam-se algumas desvantagens, mas que são superadas facilmente pelos benefícios decorrentes do uso dos cartões. Algumas vantagens que podem ser citadas são:

- assinatura, criptografia, decriptografia e geração de chaves assimétricas realizadas pelo co-processador criptográfico do cartão;
- garantia de confidencialidade da chave privada, uma vez que esta nunca deixa o cartão;
- portabilidade e armazenamento seguro de chaves e certificados;
- múltiplas aplicações em um mesmo cartão;
- duplo fator de segurança, "o que você tem" mais "o que você sabe";
- múltiplas formas de identificação em um único dispositivo: *chip*, foto, código de barras, tarja magnética, assinatura, além de identificação textual do nome indivíduo e/ou empresa;
- fácil aceitação da tecnologia por parte das pessoas, uma vez que estas já estão acostumadas a portar diversos tipos de cartões.

Algumas desvantagens também podem ser citadas:

- aumento dos custos de desenvolvimento, manutenção e gerenciamento da PKI;
- necessita de leitores especiais ainda não disponíveis em todos os computadores;
- em caso de perda, roubo ou danificação do cartão, documentos encriptados com a chave pública podem nunca mais serem recuperados (se a PKI não implementar um esquema de recuperação de chaves).

Assim como os *smart cards* intensificam a infra-estrutura de chave pública, a PKI também intensifica o uso dos smart cards, pois pode utilizar a totalidade das suas capacidades, usufruindo ao máximo dos benefícios que esta tecnologia pode oferecer.

4. O Modelo Proposto

O modelo desenvolvido possui alguns componentes de software que têm como objetivo integrar facilmente a tecnologia *smart card* a uma PKI. Assim, um desenvolvedor com o mínimo de conhecimento sobre este tipo de *token* poderá utilizar este componente em seu software sem precisar se preocupar com as questões de implementação relativas ao cartão. Estes componentes serão compostos de classes que oferecerão, a princípio, os serviços de autenticação e assinatura digital, utilizando-se de certificados de chave pública.

Para que isto seja possível, é necessário desenvolver um aplicativo de personalização e gerenciamento dos cartões. Esta aplicação será a responsável pela gravação dos dados do usuário (portador), do emissor e demais informações pertinentes ao próprio, nos cartões. Além disso, pretende-se desenvolver também, funções de manutenção destes dados, como atualização de chaves e certificados.

O modelo apresentado neste artigo não baseia-se em nenhum modelo existente, visto que este tipo de implementação normalmente não é divulgado publicamente, pois é desenvolvido por empresas que tem por objetivo, alcançar um diferencial competitivo no mercado, apresentando produtos e serviços com um maior nível de segurança que seus concorrentes. Portando, um diferencial que se pode destacar quanto a este trabalho, é que ele apresenta um modelo aberto desenvolvido em uma linguagem padrão e facilmente interpretável, a UML (*Unified Modelling Language*).

Na seção seguinte, será apresentado um exemplo de cenário de uso para aplicação do modelo proposto. Este cenário é descrito com o intuito de apresentar os requisitos e as regras de negócio ao qual serviram de base para o desenvolvimento do modelo.

4.1. Exemplo de Cenário para Aplicação

Considere o caso de uma empresa que possui uma PKI e possui o interesse de torná-la mais segura e flexível através da utilização de *tokens* criptográficos. Considere ainda que a própria empresa é a Autoridade Certificadora, gerenciando a infra-estrutura e emitindo certificados para seus colaboradores (funcionários, clientes e fornecedores). Suponha que a referida empresa ainda não sabe qual a tecnologia melhor atende as suas necessidades, e deseja realizar testes com diversos *tokens* e produtos disponíveis no mercado. A proposta aqui apresentada seria muito interessante para esta empresa, pois de forma simples e rápida ela poderá realizar testes com alguns usuários e verificar a viabilidade da tecnologia *smart card* para atender as suas necessidades.

A idéia é que o processo de distribuição dos tokens funcione da seguinte forma: quando um novo funcionário é admitido na empresa, este é cadastrado na PKI e recebe seu *smart card*, contendo seus dados de identificação pessoal (par de chaves criptográficas, certificado digital, CPF, nome, código de matrícula, etc), informações de identificação da empresa (CNPJ, chave pública, certificado, etc), além de informações sobre o próprio cartão. O mesmo processo ocorre com os clientes e fornecedores que necessitarem comunicar-se de forma segura com a empresa.

Como exemplos de utilização das funcionalidades pode-se citar: assinatura de e-mails, e documentos em geral; autenticação para acesso a sistemas da empresa, rede local, VPN (*Virtual Private Network*); e acesso físico a portas ou catracas.

4.2. Metodologia de Desenvolvimento

Este artigo é um trabalho de pesquisa de caráter empírico, pois baseia-se em relatos (através de artigos) de implementações realizadas em diversas organizações e, em constatações oriundas dos estudos realizados. Além disso, também utiliza um conhecimento que é caracterizado como senso comum que, neste caso, são certas funcionalidades ou requisitos que um determinado sistema deve possuir.

Como base teórica para o desenvolvimento deste trabalho foram utilizados livros e artigos científicos, sobre *smart cards*, PKI, criptografia e aspectos de segurança em TI relacionados com o contexto estudado. Foram considerados também, artigos técnicos e manuais de instituições de comprovado renome na comunidade acadêmica e profissional, como por exemplo IBM e Sun Microsystems.

A análise e o projeto do modelo foram feitos utilizando o paradigma de orientação a objetos e, usou-se a linguagem UML para a construção dos diagramas. O fato de a UML ser a notação padrão da OMG (*Object Management Group*) para o desenvolvimento de sistemas orientados a objetos, e o fato de existirem inúmeras ferramentas *case* disponíveis para esta linguagem como softwares livres, foram as razões que determinaram a sua escolha para a diagramação deste trabalho [Booch, Rumbaugh e Jacobson 2000].

5. Especificação do Modelo

Nesta seção é apresentada a proposta de um modelo de software que visa proporcionar a utilização da tecnologia *smart card* em uma infra-estrutura de chave pública, tendo como objetivo intensificar a segurança das chaves privadas e proporcionar maior flexibilidade a PKI. Como foi citado anteriormente, este componente de software oferecerá somente os serviços de autenticação e assinatura digital. A figura 1 apresenta os casos de uso do modelo proposto.

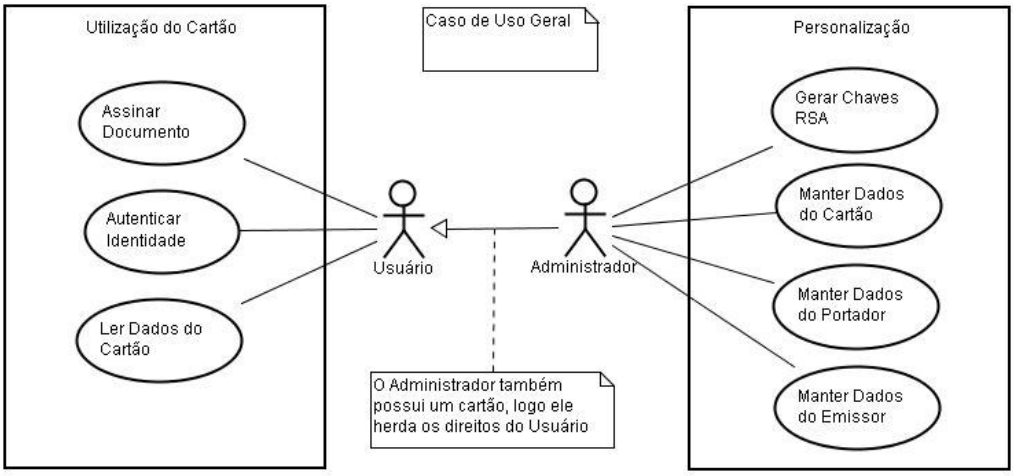

Figura 1: Diagrama de Casos de Uso

A seguir serão descritos cada um dos elementos apresentados no pelo diagrama da figura 1.

5.1. Especificação dos Atores

Portador do Cartão: entidade final da PKI, utiliza o cartão para autenticar-se e assinar digitalmente e-mails e outros documentos nos softwares da empresa, garantindo a integridade e tornando estas informações não-repudiáveis.

Administrador: responsável pelo processo de personalização dos cartões antes de estes serem entregues aos portadores (usuários). A manutenção do ciclo de vida do cartão, e das informações contidas nele, também são responsabilidades do administrador. Exemplo: atualização de um certificado digital, atualização dos dados do emissor, etc.

5.2. Especificação dos Casos de Usos

O processo de gravação dos dados no *smart card* é chamado de personalização. A etapa de personalização é um ponto crítico da vida útil do cartão: todos os cuidados de segurança devem ser aplicados para garantir a que os dados inseridos no cartão sejam íntegros e corretos. Deve-se dar atenção especial ao momento da geração das chaves de criptografia assimétrica (RSA), processo que é realizando dentro do próprio cartão. Para eliminar riscos de ataques, recomenda-se que a personalização seja feita em uma máquina isolada (sem acesso a qualquer tipo de rede) e em um ambiente físico seguro.

Gerar Chaves RSA: processo de geração das chaves criptográficas, realizado dentro do *smart card,* baseado no algoritmo RSA (Rivest, Shamir e Adleman). A aplicação *desktop* envia o tamanho de chave requerida (512, 1024, 2048 bits, por exemplo) e o *applet* do cartão calcula as chaves, retornando somente a chave pública.

Manter Dados do Cartão: aplicação *desktop* envia ao *applet* do *smart card* os dados referentes ao próprio cartão, como Identificador, PIN, Validade, Situação, etc. Os dados são armazenados no sistema de arquivos do cartão.

Manter Dados do Portador: o aplicativo desktop envia ao applet do *smart card* os dados referentes ao portador do cartão, como CPF, nome, par de chaves RSA (se estes não foram gerados pelo próprio cartão), certificado digital, etc. Os dados são armazenados no sistema de arquivos do cartão.

Manter Dados do Emissor: o aplicativo desktop envia ao applet do *smart card* os dados referentes ao emissor do cartão, como CNPJ, nome, chave pública, certificado digital, etc. Os dados são armazenados no sistema de arquivos do cartão.

Uma observação relevante: para os casos de uso a baixo, assume-se que, antes de ser executada a funcionalidade, uma conexão segura foi estabelecida entre o aplicativo servidor (*host*) e o terminal de interface com o cartão (leitor) - esta conexão segura não é foco deste trabalho. Assume-se também, que o usuário foi autenticado pelo cartão através da digitação e validação do PIN (*Personal Identification Number*).

Assinar Documento: o usuário solicita que um determinado documento seja assinado digitalmente usando a sua chave privada que está armazenada dentro do seu cartão. O aplicativo desktop realiza uma operação de *hash* sobre os dados (usando o algoritmo SHA-1 ou MD5 por exemplo), gerando um resumo de mensagem; este resumo é enviado para o cartão juntamente com o pedido de assinatura. De posse da chave privada do usuário, o cartão realiza a cifragem do resumo (utilizando RSA) e o devolve para a aplicação. O resumo cifrado agora recebe o nome de assinatura digital. A aplicação anexa a assinatura ao documento original do usuário, finalizando o processo.

Autenticar Identidade: Autenticação baseada em desafio-resposta. O aplicativo desktop gera e armazena um desafio (um número aleatório utilizando um função geradora de números pseudo-aleatórios) e envia-o para o cartão. O applet do cartão assina digitalmente o desafio e o devolve para a aplicação juntamente com o certificado digital do portador. O aplicativo verifica o certificado e valida a assinatura, comparando o desafio assinado com o enviado.

Ler Dados do Cartão: A aplicativo desktop solicita ao applet do cartão uma consulta a determinada informação armazenada em seu sistema de arquivos, especificando a entidade e dado requerido (exemplo: USUARIO + CERTIFICADO). Deixa-se claro aqui que apenas informações públicas estarão disponíveis para consulta, como por exemplo: nome e certificado digital das entidades, estado e validade do cartão, etc.

5.3. Diagrama de Classes

A figura 2 ilustra o diagrama de classes conceitual do modelo proposto, onde são apresentadas as seis classes que representam as entidades que serão modeladas quando da implementação deste trabalho e que estão presentes no cenário de utilização do sistema, sejam elas reais (Emissor, Usuário, Administrador e Cartão) ou abstratas (Serviço e ChaveRSA).

Pode-se notar no diagrama que ocorre uma divisão entre as classes, isto é, algumas classes relacionam-se com outras de forma que elas não podem separadas em pacotes ou subsistemas diferentes. As classes Serviço e Adm executarão no ambiente do cliente, e as demais classes serão executadas internamente pelo cartão. Uma descrição sobre a funcionalidade de cada classe é apresentada a seguir.

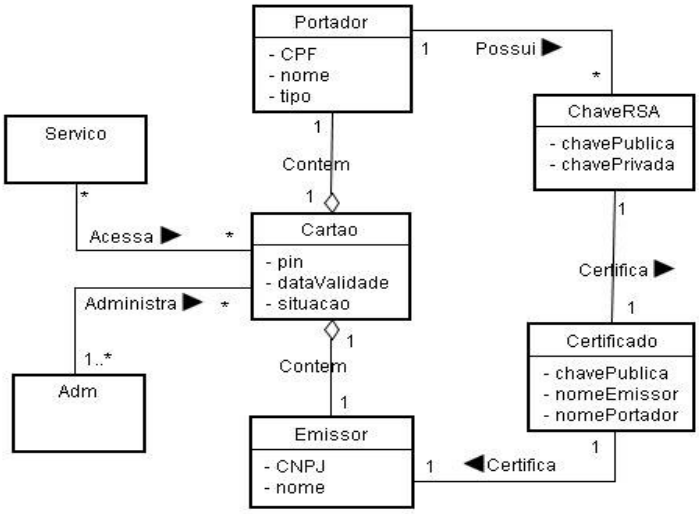

Figura 2: Diagrama de classes conceitual

Adm: será encarregada de encapsular as funções de manutenção dos dados internos do cartão, como inclusão, alteração e exclusão de informações do Emissor, Portador (usuário) e do próprio cartão.

Serviço: encapsulará as funções de utilização prática do cartão, isto é, as funções que serão utilizadas pelo usuário de forma a usufruir os benefícios do cartão.

Cartão: classe responsável por comunicar-se com as outras classes internas ao cartão e implementar a interface de comunicação entre as classes Adm e Serviço.

Portador: tem a finalidade se ler e gravar os dados do portador do cartão.

Emissor: tem a finalidade se ler e gravar os dados do emissor do cartão.

ChavesRSA: classe encarregada de manter as chaves assimétricas do portador.

Certificado: classe responsável por ler e gravar o certificado digital de cada chave pública armazenada no cartão.

O modelo de classes apresentado permite que cada portador possua mais de um par de chaves criptográficas, cada uma para um fim específico, conforme recomendam as melhores práticas de segurança em uma PKI. Por exemplo, o usuário pode ter uma chave exclusiva para autenticação e outra apenas para assinatura digital.

Não é objetivo deste trabalho abordar a geração de certificados digitais, de forma a assumir que após a geração das chaves criptográficas, a chave pública será enviada a AC (seja esta interna ou externa a organização), que se encarregará de gerar o referido certificado. Após ser entregue pela AC, o administrador encarrega-se de gravar o certificado no cartão.

A figura 3 ilustra a divisão das classes em pacotes específicos de acordo com a finalidade. O pacote CartaoApplet executará dentro do cartão, enquanto os demais serão executados na estação cliente. O pacote CartaoAdm, por possuir métodos administrativos deverá estar presente apenas na estão responsável pela personalização dos cartões, ao contrário do pacote CartaoUtil, que deverá estar instalado em todas as estações que necessitarem realizar comunicação com os *smart cards*.

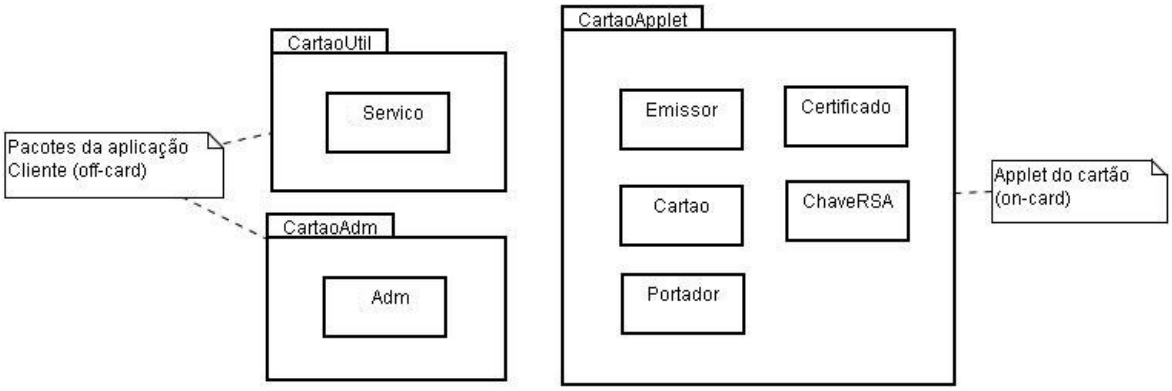

Figura 3: Pacotes de classes do sistema

Para a futura implementação deste modelo, pretende-se utilizar a linguagem JavaCard, pois após os estudos realizados verificou-se que esta plataforma é referenciada por quase todos os autores e profissionais da área, o que demonstra a sua credibilidade. Além disso, a quantidade de cartões fabricados para suportar a máquina virtual JavaCard vem crescendo significantemente, e por ser derivada da linguagem Java, JavaCard possui um número grande de desenvolvedores e sua documentação é de fácil acesso através da Internet, conseqüentemente apresenta uma maior facilidade para o desenvolvimento de trabalhos experimentais e acadêmicos.

6. Conclusão

Com a popularização dos *smart cards* e a crescente utilização de infra-estruturas de chave pública, é interessante que exista um modelo aberto e de fácil entendimento que aborde a utilização destes dispositivos em uma PKI, de forma que alguém interessado no assunto possa consultá-lo e ter uma base para desenvolver a sua própria aplicação.

Para resolver o problema do armazenamento e replicação de chaves criptográficas no usuário final de uma PKI, este artigo propôs a utilização de *smart cards*, e apresentou um modelo orientado a objetos para a aplicação destes dispositivos em uma PKI. O modelo proposto diferencia-se por ser aberto e de fácil compreensão, pois utiliza os conceitos da orientação a objetos para definir seus componentes, o que torna a modelagem mais próxima da realidade. Além disso, este trabalho contribui para esclarecer as questões relativas aos benefícios de se aplicar a tecnologia *smart card*

em uma infra-estrutura de chave pública. E através do modelo apresentado procura definir como isto deve ser feito.

Para consolidar os estudos realizados, em um trabalho futuro, pretende-se desenvolver a implementação do modelo proposto a fim de validá-lo na prática.

Uma PKI corretamente implementada e bem gerenciada, representa o estado da arte em termos de segurança para a criptografia de chave pública. A utilização de um token criptográfico contribui para agregar mais valor a PKI, aumentando significantemente o nível de segurança dos serviços oferecidos na infra-estrutura. A tecnologia *Smart Card* mostra-se o meio ideal para proporcionar versatilidade e maior segurança a PKI, pois é um dispositivo seguro e altamente difícil de ser falsificado ou adulterado.

Referências

Burnett, Steve., Paine, Stephen. (2002) "Criptografia e Segurança: O Guia Oficial RSA", Rio de Janeiro, Editora Campus, 365p.

Booch, G., Rumbaugh, J., Jacobson, I. (2000) "UML – Guia do Usuário", Rio de Janeiro, Editora Campus, 472p.

DatacardGroup (2001), "The Transition to Multi-application Smart Cards", http://www2.datacard.com/downloads/pdf/white_paper_transition.pdf, Maio.

Dreifus, Henry N., Monk, J. Thomas (1998) "Smart Cards : A Guide to Building and Managing Smart Card Applications", New York, John Wiley & Sons, 328p.

Hamann, E.-M., Henn, H., Schäck, Thomas. Seliger, F. (2001) "Securing e-business applications using smart cards", IBM Systems Journal, Vol 40, No 3. http://www.research.ibm.com/journal/sj/403/hamann.html, Abril.

Mehdizadeh, Yahya (2004) "Convergence of Logical and Physical Security", SANS Institute, http://www.sans.org/rr/papers/6/1308.pdf, Março.

Keith, Angela (2003) "Common issues in PKI implementations - climbing the 'Slope of Enlightenment'", GSEC Practical v.1.4b, SANS Institute. http://www.sans.org/rr/papers/index.php?id=1198, Março.

Kiran, S. Lareau, P., Loyd, Steve. (2002) "PKI Basics – A Technical Perspective", PKI Forum, http://www.pkiforum.org/whitepapers.html, Março.

Longo, E., Stapleton, J. (2002) "PKI Note – Smart Cards", PKI Forum, http://www.pkiforum.org/whitepapers.html, Março.

Schneier, Bruce (1996) "Applied Cryptography", Second Edition, Nova York, John Wiley & Sons Inc., 758p.