

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CURSO DE BACHARELADO EM CIÊNCIA DA
COMPUTAÇÃO**

Carlos Francisco Tatara

S2Card

Trabalho de Conclusão de Curso de Graduação apresentado à Universidade Federal de Santa Catarina para a obtenção do grau de Bacharel em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.

Orientador

custodio@inf.ufsc.br

Florianópolis, Fevereiro de 2003

S2Card

Carlos Francisco Tatara

Este Trabalho de Conclusão de Curso de Graduação foi julgado adequado para a obtenção do título de Bacharel em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.

Orientador

custodio@inf.ufsc.br

Prof. José Mazzucco Junior, Dr.

Coordenador do Curso

mazza@inf.ufsc.br

Banca Examinadora

Prof. Júlio da Silva Dias, M.Sc

jdias@inf.ufsc.br

Fabiano Goellner dos Santos

goellner@inf.ufsc.br

XWMQWW
ALFLZNH
UOTQWLF
RZALANF
UF

Para meus pais, Nilson e Alacir e meus irmãos Daniel e
Fernando que são de fundamental importância na minha
vida.

Agradecimentos

Agradeço a Universidade Federal de Santa Catarina e ao Departamento de Informática e Estatística.

Agradeço ao professor Ricardo Custódio por ter me dado a oportunidade de trabalhar nesse projeto.

Ao Júlio da Silva Dias e ao Fabiano Goellner dos Santos que fazem parte da equipe do Projeto S2Card.

Aos amigos que durante os anos de graduação compartilharam das mesmas alegrias e frustrações dentro do curso.

Conteúdo

Lista de Figuras	ix
Lista de Tabelas	x
Lista de Siglas	xi
Resumo	xii
Abstract	xiii
1 Introdução	1
1.1 Motivação	1
1.2 Objetivos Gerais	1
1.3 Objetivos Específicos	2
1.4 Materiais e Métodos	2
1.5 Organização do Texto	2
2 Tecnologia de Cartões	3
2.1 Introdução	3
2.2 Resumo Histórico	3
2.3 Tipos de Cartões	7
2.3.1 Cartões com Tarja Magnética	7
2.3.2 SmartCards	9
2.3.3 Cartões de Memória Ópticos	15
2.4 Conclusão	16

3	Fundamentos da Criptografia	17
3.1	Introdução	17
3.2	Criptografia Simétrica	18
3.3	Criptografia Assimétrica	19
3.4	Função Resumo	20
3.5	Certificado Digital	21
3.6	Assinatura Digital	22
3.7	PDDE	23
3.8	Conclusão	24
4	Documento Eletrônico	25
4.1	Introdução	25
4.2	Definição	25
4.3	Validade Jurídica de Documentos Eletrônicos	26
4.4	Conclusão	27
5	S2Card	28
5.1	Introdução	28
5.2	Modelo Atual de Assinatura Digital com SmartCards	28
5.3	Modelo Proposto	29
5.4	JavaCard	32
5.4.1	Definição	32
5.4.2	Ciclo de Desenvolvimento de um applet para JavaCards	32
5.5	OpenCard framework	33
5.6	Implementação	34
5.6.1	Applet de controle do SmartCard	34
5.6.2	Sistema do Terminal	35
5.7	Funcionamento	35
5.8	Conclusão	39
6	Conclusão	40

Referências

Bibliográficas

41

A Anexos

43

Lista de Figuras

2.1	Cartão de Metal	4
2.2	Descrição das Trilhas da Tarja Magnética	8
2.3	SmartCard com contato	10
2.4	SmartCard sem contato	10
2.5	SmartCard Híbrido	11
2.6	Dimensões de um SmartCard	12
3.1	Processo de cifragem e dedifragem	18
3.2	Processo de cifragem e decifragem usando criptografia simétrica	19
3.3	Processo de cifragem e decifragem usando criptografia assimétrica	19
3.4	Estrutura de um Certificado Digital	22
3.5	Processo de Assinatura e Verificação de Assinatura Digital utilizando RSA	23
3.6	Esquema de funcionamento da Protocolizadora Digital de Documentos Eletrônicos	24
5.1	Modelo Atual de Assinatura Digital com SmartCards	29
5.2	Processo de Assinatura no Modelo Proposto	32
5.3	Ciclo de Desenvolvimento de um Applet	33
5.4	Tela inicial de assinatura	35
5.5	Tela de solicitação de inserção do SmartCard	36
5.6	Tela de solicitação do PIN do usuário	37
5.7	Processo de assinatura digital em andamento	38

Lista de Tabelas

2.1	Principais eventos na história do desenvolvimento da tecnologia de cartões	6
2.2	Função de cada contato do SmartCard	13

Lista de Siglas

AC - Autoridade Certificadora

APDU - Application Data Unit

API - Application Programming Interface

AIDC - Automatic Identification and Data Capture

BART - Bay Area Rapid Transit

CPU - Central Process Unit

DES - Data Encryption Standard

EEPROM - Electronic Erasable Programmable Read Only Memory

ISO - International Organization for Standardization

OFC - OpenCard Framework

PCMCIA - Personal Computer Memory Card International Association

PDDE - Protocolizadora Digital de Documentos Eletrônicos

PTT - Postal and Telecommunications Services

PIN - Personal Identification Number

RAM - Random Access Memory

ROM - Read Only Memory

RSA - Iniciais de Ron **R**ivest, Adi **S**hamir e Len **A**dleman

Resumo

Este trabalho descreve um novo modelo de assinatura digital utilizando SmartCards proposto pelo Laboratório de Segurança em Computação da Universidade Federal de Santa Catarina.

Na proposta, o cartão passa a ter autonomia para decidir se pode ou não assinar um documento. Essa decisão é tomada com base numa lista de tipos de documentos que o cartão possui.

Outra inovação é a inclusão de um banco de dados de registros de assinaturas no modelo. Isso permite ao usuário ter um controle completo sobre os documentos que assinou.

Além de poder decidir sobre a ação de assinar um documento, o SmartCard também tem controle sobre a integridade do banco de dados (BD). Este controle é feito por meio do armazenamento de um resumo do BD que é atualizado toda vez que um novo documento é assinado. A comparação entre o resumo atual do BD e o resumo presente no SmartCard permite saber se os dados dos registros de assinaturas permanecem consistentes.

Palavras chaves: SmartCard, S2Card, assinatura digital, criptografia.

Abstract

This work describes a new model of digital signature using SmartCards considered for the Computer Security Lab of the Federal University of Santa Catarina.

In this proposal, the card starts to have autonomy to decide if it can or not sign a document. This decision is taken with base in one list of types of documents that the card possess.

Another innovation is the inclusion of a data base of registers of signatures in the model. This allows the user to have a complete control on the documents that it signed.

Beyond being able to decide on the action to sign a document, the SmartCard also has control on the integrity of the data base (BD).

This control is made by means of the storage of a hash of the BD that is brought up to date all time that a new document is signed.

The comparison enters the current hash of the BD and the present hash in the SmartCard allows to know if the data of the registers of signatures remain consistent.

Keywords: SmartCard, S2Card, digital signature, cryptography.

Capítulo 1

Introdução

O projeto S2Card é desenvolvido no Laboratório de Segurança em Computação da Universidade Federal de Santa Catarina e está ligado ao projeto do Cartório Virtual.

1.1 Motivação

O crescente uso de documentos eletrônicos trouxe à tona o problema de sua validade jurídica. O uso da assinatura digital é um meio seguro de se autenticar documentos eletrônicos. Porém a portabilidade do certificado digital é um problema, pois normalmente o certificado fica armazenado no disco rígido do computador do usuário. O uso de SmartCards para armazenar o certificado digital apresenta-se como uma solução tecnologicamente viável.

Outra necessidade é a de se ter meios de se manter um registro confiável dos documentos assinados.

1.2 Objetivos Gerais

- Desenvolver um novo modelo de assinatura digital de documentos utilizando SmartCards.
- Criar um mecanismo que permita ao usuário ter maior controle sobre os documentos

que assinou.

1.3 Objetivos Específicos

- Estudar o funcionamento dos SmartCards.
- Buscar técnicas mais eficientes de programação nos SmartCards.

1.4 Materiais e Métodos

Inicialmente foi realizado um estudo sobre cartões em geral, sua história, funcionamento e tecnologia.

Num segundo momento foi feito um estudo mais aprofundado sobre SmartCards.

Optou-se pelo uso de SmartCards do tipo JavaCard.

Passou-se a estudar as técnicas e ferramentas de programação para este tipo de cartão.

Posteriormente iniciou-se o estudo do OpenCard Framework, que é utilizado para desenvolver aplicativos que interajam com o SmartCard.

1.5 Organização do Texto

O texto está organizado da seguinte forma: no capítulo 2 é apresentada a tecnologia de cartões, um breve histórico do seu uso e os tipos atualmente encontrados no mercado. No capítulo 3 é feita uma breve descrição dos principais fundamentos de criptografia, o capítulo 4 traz as definições de documento e discute sobre a validade jurídica de documentos eletrônicos. O capítulo 5 apresenta o projeto S2Card, suas características, funcionamento e a sua implementação.

Capítulo 2

Tecnologia de Cartões

2.1 Introdução

Uma forma de identificação, um meio de proporcionar aos clientes melhores serviços, um objeto para facilitar o controle de acesso a determinados lugares, enfim, um cartão pode ser definido como algo que fornece acesso a alguma coisa e possui alguma tecnologia de AIDC (Automatic Identification and Data Capture) como por exemplo, código de barras, impressão digital ou tarja magnética.

O material usado em sua fabricação pode variar (plástico, PVC, papel, metal), bem como a sua finalidade (Cartões Financeiros, Cartões de Controle de Acesso, Cartões de Identificação), mas o fato é que com o avanço na tecnologia de fabricação, e nas ferramentas de segurança, os cartões tornaram-se objetos indispensáveis para boa parte da população.

2.2 Resumo Histórico

A necessidade de facilitar a identificação de clientes, e o desejo das empresas de oferecer facilidades e melhores serviços aos consumidores deu origem ao uso de cartões na área comercial e financeira no início do século 20.

Inicialmente feitos de metal (Figura 2.1), os cartões de débito foram usados pela primeira

vez pela Western Union em 1914 e tinham como objetivo dar aos seus clientes preferenciais um prazo maior para o pagamento dos serviços usados.



Figura 2.1: Cartão de Metal

Esse tipo de cartão ficou conhecido na época como Dinheiro de Metal. Até o início da Segunda Guerra Mundial, diversos setores do comércio passaram a usá-lo. Durante a guerra o uso de cartões no comércio foi restringido, devido as preocupações inerentes da época.

Como forma de identificação, um fato de grande relevância foi a emissão em 1937 pelos EUA do cartão de seguro social.

Com o final da guerra, os cartões de crédito tornaram-se mais acessíveis ao público geral, principalmente com o início de seu uso pelos bancos. O primeiro a entrar nesse mercado foi o Franklin National Bank de Nova Iorque em 1951. O sistema de débito funcionava de maneira muito similar à de hoje. O consumidor fazia a compra usando cartão; o comerciante obtinha autorização do banco e efetuava a venda. O banco reembolsava o comerciante e efetuava o débito na conta do consumidor numa data posterior.

Com o sucesso obtido pelo Franklin National Bank, diversas outras instituições financeiras passaram a criar seus sistemas de cartões de crédito. Em 1950 o Diners Club lançou o seu cartão de débito, que tinha como público alvo homens de negócio e suas despesas com viagens e entretenimento. O Diners Club dava para seus membros um prazo de 60 dias para efetuar o pagamento.

As associações de cartões surgiram em 1965, quando o Bank of America firmou acordos de licença com outros bancos. O objetivo dessas associações era a

diminuição de custos operacionais o que permitiu que pequenas instituições financeiras também pudessem fazer uso do sistema de cartões. No final da década de 60 existiam duas grandes associações de cartões: BankAmericard e MasterCharge.

Com a intenção de explorar o mercado fora dos EUA, em 1977 a BankAmericard mudou o nome para Visa, e em 1979 a MasterCharge passou a se chamar MasterCard.

O uso de microchips embutidos e novas tecnologias de segurança, deram aos cartões um maior campo de atuação. Fora da área financeira, o seu uso também é significativo. Cartões de Acesso, Carteira de Motorista, Cartões de CPF e Carteiras de Estudante são apenas alguns exemplos.

A Tabela 2.1 mostra os principais eventos na história do desenvolvimento da tecnologia de cartões.

Tabela 2.1: Principais eventos na história do desenvolvimento da tecnologia de cartões

Ano	Evento
1914	Cartões de Débito - Wester Union - "Dinheiro de Metal"(EUA)
1937	Emissão do primeiro cartão de seguro social (EUA)
1951	Primeiro cartão de crédito - Franklin National Bank (EUA)
1960	Departamento de Trânsito de Londres usa tarja magnética nos tickets do metrô
1968	Jurgen Dethloff e Helmut Grotrupp patentaram os primeiros cartões com circuitos integrados (Alemanha)
1973	Estabelecidos padrões para as tarjas magnéticas
1976	SmartCard desenvolvido pela companhia de computadores Citi Honeywell Bull. (França)
1978	Estabelecidos padrões para SmartCards
1983	Deutsche Bundespost realiza estudo da tecnologia de SmartCards para sistemas de telefonia. (Alemanha)
1983	Departamento de Defesa dos EUA testa SmartCards para uso em sistemas de identificação.
1994	Estabelecidos padrões cartões de memória ópticos.
1996	Estabelecidos padrões para tarjas magnéticas de alta coercividade
1996	1,5 milhões de SmartCards sem contato são emitidos na Coreia do Sul para uso no sistema de transporte coletivo.
1996	SmartCards usados nos Jogos Olímpicos de Atlanta(EUA) no comércio local.

2.3 Tipos de Cartões

Atualmente existem 3 tecnologias principais no campo de cartões: Cartões com Tarja Magnética, SmarCards e Cartões de Memória Ópticos.

2.3.1 Cartões com Tarja Magnética

2.3.1.1 Resumo Histórico

O primeiro uso de tarjas magnéticas em cartões foi feito pelo Departamento de Trânsito de Londres no início dos anos 60 para controlar o acesso ao Metrô da cidade (London Underground).

No final desta mesma década o BART(Bay Area Rapid Transit)(EUA) instalou um sistema de tickets que tinham o mesmo tamanho dos cartões de crédito atuais. O sistema usava um valor armazenado na tarja que era lido e reescrito a cada vez que o cartão era usado.

Os primeiros cartões de crédito com tarja magnética foram emitidos em 1951, mas apenas a partir da década de 70 é que os padrões de fabricação começaram a ser estabelecidos. Hoje, todos os cartões financeiros seguem padrões ISO para assegurar o seu uso em todo o mundo.

2.3.1.2 Características Físicas

Os Padrões ISO 7810,7811 e 7813 descrevem as características dos Cartões com Tarja Magnética. A tarja magnética é feita de pequenas partículas magnéticas. De acordo com esses padrões a tarja do cartão tem 3 trilhas magnéticas.

As trilhas são codificadas a técnica de gravação F/2F, onde pulsos de clock ocorrem em intervalos regulares. Uma mudança de fluxo entre os clocks significa o bit 1, e a ausência dessa transição significa o bit 0. A figura 2.2 mostra a descrição das 3 trilhas da tarja magnética.

TRILHA 1	
Capacidade	79 caracteres, incluindo o caractere indicador de início e o caractere LRC
Densidade de bits	8,27 bits por milímetro
Codificação	6 bits mais um de paridade. (64 caracteres diferentes)
Conjunto de Caracteres	Espaço ! " # \$ % & ' () + , - . / 0 1 2 3 4 5 6 7 8 9 ; < = > A B C D E F G H I J K L M N O P Q R S T U V W X Y X [\] ^ _
Caractere Indicador de Início	%
Caractere Indicador de Final	?
Caractere Separador	^
Apenas caracteres maiúsculos são permitidos na Trilha 1. Caracteres minúsculos são automaticamente convertidos para maiúsculo	
TRILHA 2	
Capacidade	40 caracteres, incluindo o caractere indicador de início e o caractere LRC
Densidade de bits	2,95 bits por milímetro
Codificação	4 bits mais um de paridade. (16 caracteres diferentes)
Conjunto de Caracteres	0 1 2 3 4 5 6 7 8 9 ; < = > ?
Caractere Indicador de Início	,
Caractere Indicador de Final	?
Caractere Separador	=
TRILHA 3	
Capacidade	107 caracteres, incluindo o caractere indicador de início e o caractere LRC
Densidade de bits	8,27 bits por milímetro
Codificação	4 bits mais um de paridade. (16 caracteres diferentes)
Conjunto de Caracteres	0 1 2 3 4 5 6 7 8 9 ; < = > ?
Caractere Indicador de Início	;
Caractere Indicador de Final	?
Caractere Separador	=

Figura 2.2: Descrição das Trilhas da Tarja Magnética

Além do fato dos cartões com tarja magnética possuírem pouco espaço para armazenamento de dados (226 caracteres no total), a robustez das informações gravadas também é um problema. O termo usado para medir o quão suscetíveis a danos são os dados armazenados na tarja é Coercividade. Medida em Oersteds(Oe), a coercividade de um cartão de crédito comum é de cerca de 300 Oe, considerada baixa coercividade (LoCo). Tarjas consideradas de alta Coercividade tem valores entre 2500 e 4000 Oe. A técnica de codificação é a mesma para os dois tipos de tarja, exceto que para escrever nos cartões com alta coercividade é necessária uma corrente elétrica mais forte no cabeçote de escrita. Leitores de tarja magnética que seguem os padrões ISO podem ler os dois tipos

de tarja. As tarjas de alta coercividade são imunes aos campos magnéticos domésticos, porém devido ao alto custo ainda não são usadas em larga escala.

2.3.2 SmartCards

2.3.2.1 Resumo Histórico

Em 1968, os inventores alemães Jürgen Dethloff e Helmut Grötrupp patentearam os primeiros cartões com circuito integrados. Projetos similares foram desenvolvidos no Japão em 1970 e na França em 1974.

Em 1984 o PTT (Postal and Telecommunications Services) da França, teve sucesso em lançar o "telephone smartcard". Desde então, os SmartCards tornaram-se largamente aceitos na Europa e recentemente começaram a entrar em cena na América com as iniciativas da American Express, Visa e MasterCard. Em 2002, o Departamento de Defesa dos EUA emitiu 4,3 milhões de cartões para controle de acesso físico e on-line.

2.3.2.2 Tipos de SmartCards

Os SmartCards podem ser classificados pela forma de transmissão de dados ou pela forma de construção.

Pela forma de transmissão de dados podem ser: Com contato, sem contato ou híbridos.

SmartCards com Contato: Este tipo de SmartCard (Figura 2.3) precisa entrar fisicamente em contato com um terminal de leitura. O cartão tem uma pequena placa dourada de cerca de 1/2 polegada de diâmetro. Quando o cartão é inserido no terminal, ele entra em contato com os conectores elétricos que transferem dados para o chip.



Figura 2.3: SmartCard com contato

SmartCards sem Contato: O cartão não precisa entrar em contato com o terminal de leitura. A transmissão de dados é feita através de sinais de rádio. O formato deste tipo de cartão é similar ao anterior, exceto pelo fato de não ter contatos externos e possuir uma antena embutida (Figura 2.4).

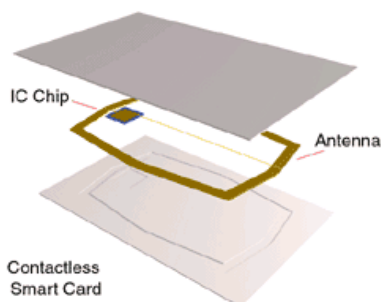


Figura 2.4: SmartCard sem contato

SmartCards Híbridos: São considerados Híbridos, os SmartCards que englobam tanto a tecnologia de transmissão de dados sem contato (por intermédio da antena), quanto a de transmissão de dados com contato. A Figura 2.5 mostra os componentes deste tipo de cartão.

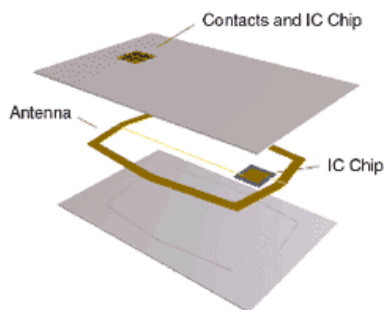


Figura 2.5: SmartCard Híbrido

Pela forma de construção podem ser: Cartões de Memória, Cartões com microprocessador, Cartões com coprocessador criptográfico.

Cartões de Memória: Possuem uma memória EEPROM e uma memória ROM, além de alguma lógica de segurança. Aplicações comuns esse tipo de cartão são: cartões de telefone pré-pago e cartões de seguro de saúde.

Cartões com microprocessador: Os componentes deste tipo de arquitetura são: CPU, RAM, ROM e EEPROM. O sistema operacional é normalmente armazenado na ROM, a CPU usa a RAM como memória de trabalho, e os dados são armazenados na EEPROM. A interface serial I/O normalmente consiste de um simples registrador, através do qual os dados são transferidos da forma "half-duplex", bit a bit.

Cartões com Coprocessador Criptográfico: Embora tecnicamente possam ser incluídos na categoria anterior, eles são separados devido às diferenças de custo e funcionalidades. Como os algoritmos de criptografia assimétrica requerem o cálculo de números inteiros grandes, um processador de 8 bits com pouca memória RAM levaria alguns minutos para executar uma operação com uma chave privada de 1024 bits. Entretanto, se um coprocessador criptográfico for adicionado a arquitetura, o tempo requerido para a mesma operação será cerca de uma centena de microssegundos. Os coprocessadores criptográficos incluem unidades aritméticas adicionais desenvolvidas especificamente para cálculos com números inteiros grandes e rápida exponenciação .

2.3.2.3 Característica Físicas e Elétricas

Um SmartCard é feito de plástico, do mesmo tamanho de um cartão de crédito, com um chip de circuito integrado embutido que pode fornecer apenas armazenamento de dados, ou armazenamento de dados com um microprocessador programável. A maioria possui uma lógica que especifica as regras de acesso de leitura e escrita na memória.

As dimensões de um SmartCard estão descritas no padrão ISO 7810. Essas dimensões são mostradas na figura abaixo (Figura 2.6).

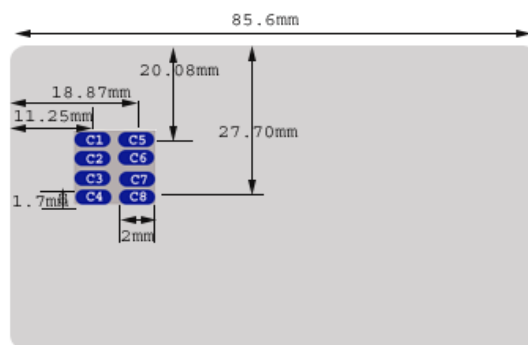


Figura 2.6: Dimensões de um SmartCard

A maioria dos SmartCards tem oito campos de contato na face frontal, entretanto dois deles são reservados para uso futuro, e muitos fabricantes produzem cartões com seis contatos para reduzir os custos de produção. Os contatos são normalmente numerados de C1 a C8. A tabela abaixo (Tabela 2.2) descreve a função de cada contato.

Tabela 2.2: Função de cada contato do SmartCard

Posição	Abreviatura	Função
C1	VCC	Suprimento de Energia
C2	RST	Reset
C3	CLK	Clock
C4	RFU	Reservado para uso futuro
C5	GND	Ground
C6	VPP	Voltagem para programação externa
C7	I/O	Comunicação Serial de Entrada e Saída
C8	RFU	Reservado para uso futuro

2.3.2.4 Transmissão de Dados

Toda a comunicação de, e para o SmartCard, é feita através do contato C7. Ela é sempre iniciada pelo terminal, o que implica em um tipo de relacionamento cliente/servidor entre o cartão e o terminal.

2.3.2.5 Fragilidades na Segurança dos SmartCards

Ataques aos SmartCards são normalmente de 2 categoria: Lógicos e Físicos.

Ataques Lógicos: Ocorrem quando o SmartCard está operando sob condições normais, mas informações sigilosas são obtidas dos bytes que entram e saem do cartão. Um exemplo disso é o chamado "ataque baseado no tempo de execução" descrito por Paul Kocher [KOC 98]. Neste ataque, vários padrões de bytes são enviados para o cartão para serem cifrados com a chave privada contida no cartão. Informações

como o tempo gasto para executar a operação e a quantidade de "0" e "1" no bytes de entrada são usados para, eventualmente, obter a chave privada.

Ataques Físicos: Ocorrem quando as condições normais, como temperatura, frequência de clock, voltagem etc, são alteradas no sentido de obter acesso a informações sigilosas do SmartCard.

Outros tipos de ataques se utilizam de falhas de projeto, e em falhas nos programas dos SmartCards.

2.3.2.6 Capacidades Criptográficas

O atual estágio de desenvolvimento dos SmartCards oferece capacidades criptográficas suficientes para suportar aplicações e protocolos de segurança populares.

Por exemplo: Suporta assinatura e verificação RSA com tamanho de chave de 512, 768 ou 1024 bits. O algoritmo tipicamente usado é o "Teorema do Resto Chinês"(CRT), no sentido de aumentar a velocidade de processamento. Mesmo com uma chave de 1024 bits, o tempo necessário para realizar a assinatura é de menos de um segundo. Normalmente o arquivo na EEPROM que contém a chave privada é designado como material sigiloso e nunca deve deixar o chip. O uso da chave privada é protegido pelo PIN do usuário.

DES e o triple DES também são comumente encontrados nos SmartCards.

2.3.2.7 Aplicações para SmartCards

- **Identificação de funcionários:** Empresas estão utilizando SmartCards como parte do seu programa de segurança.
- **Controle de Acesso:** O controle de acesso físico a edifícios e a outros ambientes, como garagens, pode ser efetuado com o uso de SmartCards. Normalmente são utilizados SmartCards sem contado.
- **PC/Network logon**

- **Assinatura Digital:** O cartão possui o certificado digital do proprietário.
- **Armazenamento seguro de informações sigilosas**
- **Transações Comerciais**
- **Autenticação para acessar Websites.**

2.3.2.8 Padrões de criptografia relacionados com SmartCards

- **PKCS11:** Define uma arquitetura padrão para componentes de hardware criptográficos, como PCMCIA e SmartCards que permitem um alto nível de segurança de dados. Este padrão especifica uma API, chamada Cryptoki, para dispositivos que mantenham informações criptográficas e executem funções de criptografia.
- **PKCS7:** Este padrão descreve a sintaxe geral para dados aos quais a criptografia pode ser aplicada. Por exemplo: Assinatura Digital e Envelope Digital.

2.3.3 Cartões de Memória Ópticos

Esse tipo de cartão usa uma tecnologia similar àquela encontrada no Cds de música ou Cd Roms. Uma pequena placa dourada feita com material sensível ao laser é inserida no cartão e usada para armazenar informações.

O material usado é composto de diversas camadas que reagem quando o feixe de laser incide diretamente sobre ele. O laser "queima" uma parte do material, fazendo uma pequena marca (2,25 microns de diâmetro). A presença ou não desta marca indica um "0" ou "1". A tecnologia atualmente usada nesse processo não permite que os dados sejam apagados fazendo dos cartões ópticos uma mídia do tipo WORM (Write Once Read Many - Escreva uma Vez Leia Várias).

A capacidade típica desse tipo de cartão varia entre 4 e 6,6 MB, o que permite o armazenamento de imagens como fotografias, impressões digitais, Raios-x etc.

2.4 Conclusão

Com quase um século de uso é inegável a utilidade dos cartões, sejam eles com tarja magnética, SmartCards ou ainda Cartões de Memória Ópticos. Aliada a sua facilidade de uso, o desenvolvimento de novas tecnologias de segurança tornaram hoje os cartões ferramentas que além de agilizar processos, garantem altos níveis de confiabilidade para os usuários.

Capítulo 3

Fundamentos da Criptografia

3.1 Introdução

A palavra criptografia vem da junção de duas palavras gregas (kriptos = escondido, oculto e grifo = escrita).

Diversos autores têm suas definições de criptografia:

Stallings [STA 98] - criptografia consiste na arte de escrever em cifras e códigos, fazendo uso de um conjunto de técnicas que tornam uma mensagem incompreensível (texto cifrado). Este processo é conhecido como cifragem. A decifragem, que é o processo inverso, consiste em transformar o texto cifrado em texto compreensível (texto plano), de tal forma que somente o destinatário consegue a informação.

Schneier [SCH 96] - criptografia pode ser definida como a arte e ciência de garantir a segurança de mensagens constantes na comunicação entre uma entidade emissora e uma entidade receptora.

Menezes [AM 96] - criptografia é o estudo de técnicas matemáticas relacionadas com os aspectos de segurança da informação como confidencialidade, integridade de dados, autenticação de entidade, e autenticação de origem de dados.

Os objetivos da criptografia segundo Menezes [AM 96] são:

Confidencialidade : Somente as entidades autorizadas terão acesso a informação.

Integridade : Os dados serão alterados somente por entidades autorizadas.

Autenticação Está relacionada com identificação. Essa função aplica-se sobre todas as entidades envolvidas no processo de criptografia.

Não-Repúdio : A entidade que realizou determinada ação não pode negá-la.

Para efetuar os processos de cifragem e decifragem, são utilizados algoritmos de criptografia. A Figura 3.1 dá uma visão geral do processo.

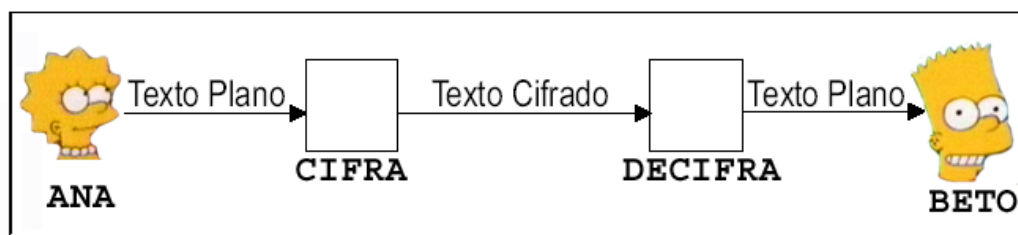


Figura 3.1: Processo de cifragem e dedifragem

3.2 Criptografia Simétrica

A característica da criptografia simétrica, também conhecida como criptografia tradicional, é uso de uma mesma chave criptográfica para cifrar e decifrar o documento. Esta chave normalmente é designada como **chave secreta**. Geralmente o algoritmo usado para cifrar e decifrar o documento é o mesmo, sendo alterada apenas a forma como a chave secreta é utilizada. A Figura 3.2 ilustra o processo de criptografia simétrica.

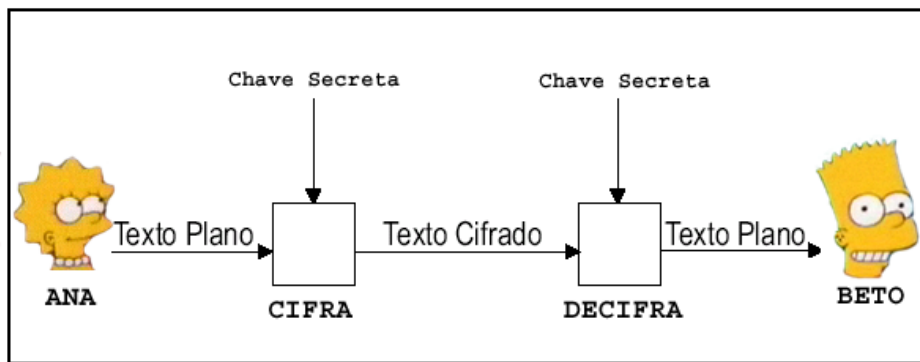


Figura 3.2: Processo de cifragem e decifragem usando criptografia simétrica

3.3 Criptografia Assimétrica

Neste sistema de criptografia, também chamado de criptografia de chave pública, utiliza-se um par de chaves (em alguns sistemas é possível utilizar mais de duas chaves). Uma delas, denominada **chave privada** é mantida sob sigilo. A outra, chamada de **chave pública** deve ser de alguma forma divulgada.

Qualquer das chaves pode ser usada no processo de criptografia, sendo que, se a chave privada for usada pra cifrar o documento, somente a chave pública poderá decifrá-lo, e vice-versa [STA 98].

A Figura 3.3 ilustra o uso de criptografia assimétrica para cifrar e decifrar um documento.

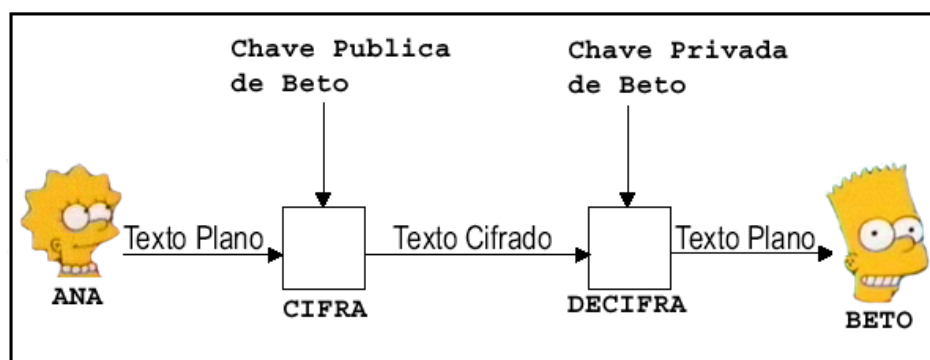


Figura 3.3: Processo de cifragem e decifragem usando criptografia assimétrica

A idéia desse tipo de criptossistema foi proposta por Whitfield Diffie e Martin Hellman [DIF 76] em 1976, e um ano depois, o primeiro algoritmo a utilizar esta técnica, o RSA [RR 76], foi apresentado. Proposto por Ron Rivest, Adi Shamir e Len Adleman o RSA é ainda hoje base da maioria das aplicações que utilizam criptografia assimétrica.

3.4 Função Resumo

Segundo Stallings [STA 98] um resumo é gerado por uma função H na forma $h = H(M)$, onde M é uma mensagem de tamanho variável e $H(M)$ é o valor de tamanho fixo do resumo de M . O principal objetivo de uma Função Resumo é obter um valor de tamanho fixo que possa identificar de forma unívoca um bloco de dados de qualquer tamanho. Ainda de acordo com Stallings[STA 98], para que se possa confiar no valor de uma Função Resumo é necessário que ela atenda a algumas características:

1. H possa ser aplicado sobre um bloco de dados de qualquer tamanho.
2. H produz um resultado de tamanho fixo.
3. $H(x)$ é relativamente fácil de computar dado qualquer x .
4. Dado qualquer valor de resumo, é computacionalmente impraticável de se chegar ao bloco de dados original.
5. Também é computacionalmente impraticável encontrar dois blocos de dados diferentes que tenham o mesmo valor de resumo.
6. É impraticável computacionalmente encontrar um par (x,y) tal que $H(x)=H(y)$. A esta característica se dá o nome de **resistência forte a colisão**.

Os principais algoritmos para obtenção de Resumo são:

MD5 [RIV 92] - Bloco de entrada de qualquer tamanho e valor de saída de 128 bits.

SHA-1 [Dep 93] - Bloco de entrada de tamanho máximo de 2 na 64 bits e saída de 160 bits.

RIPEND-160 [Thi 96]- Bloco de entrada de qualquer tamanho e saída de 160 bits.

3.5 Certificado Digital

Um certificado digital é um arquivo emitido por um entidade confiável conhecido como AC (autoridade certificadora), que contém informações sobre uma pessoa física ou jurídica. Cabe às ACs estabelecer a identidade das pessoas ou organizações para quem emitem os Certificados Digitais.

O formato mais conhecido e largamente aceito de certificados digitais é a recomendação ITU-T X.509v3.

A figura 3.4 ilustra de forma simplificada a estrutura dos dados de um certificado digital[PAS 01].

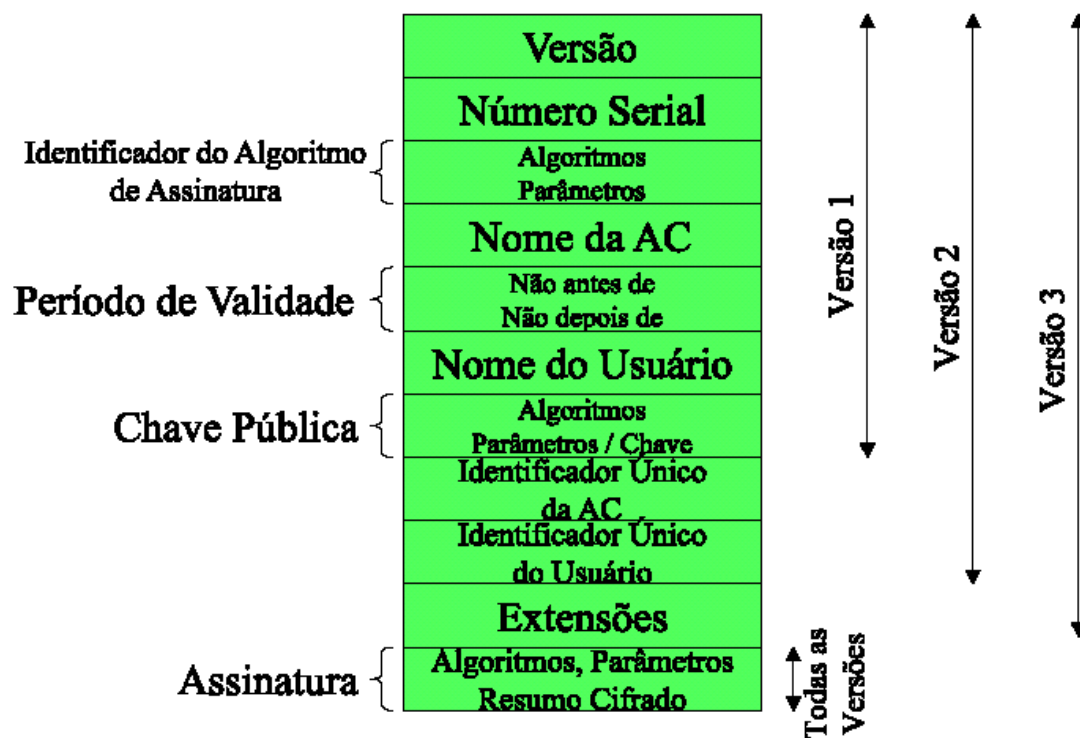


Figura 3.4: Estrutura de um Certificado Digital

3.6 Assinatura Digital

Assinatura digital é uma seqüência de bits que identifica o autor de um documento, garantindo também a integridade das informações nele contidas. A assinatura é obtida através do uso de técnicas criptográficas:

- Uso de funções de resumos
- Uso de algoritmos de assinatura digital
- Utilizando o conceito de chaves públicas

A ilustração abaixo 3.5 é baseada na figura do livro de William Stallings [STA 98] página 312, e dá uma visão geral do processo de assinatura e verificação de assinatura digital utilizando o algoritmo RSA.

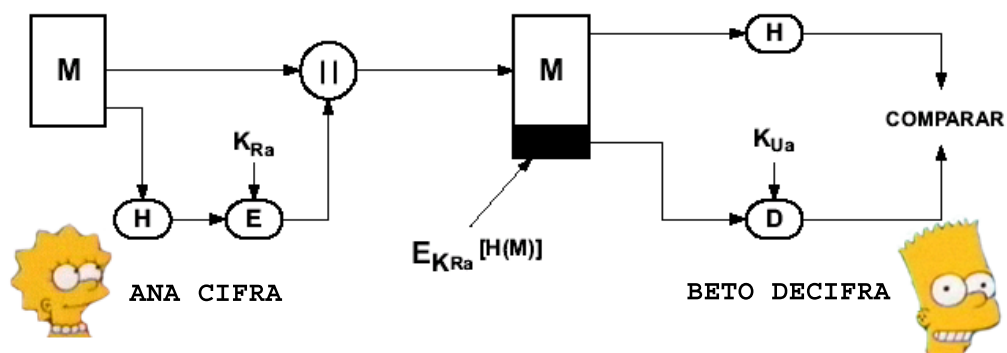


Figura 3.5: Processo de Assinatura e Verificação de Assinatura Digital utilizando RSA

- Ana deseja enviar uma mensagem (M) assinada para Beto;
- Ana calcula o Resumo da mensagem (H) e cifra usando a sua chave privada(K_{Ra});
- O resultado é concatenado com M e enviado para Beto;
- Quando Beto recebe a mensagem, calcula Resumo de M e compara com o resultado da decifragem de $E_{K_{Ra}}[H(M)]$ usando a a chave pública de Ana;
- Se os resultados forem iguais, significa que a mensagem foi escrita de fato por Ana, e não foi alterada.

3.7 PDDE

Uma Protocolizadora Digital de Documentos Eletrônicos tem a função de fornecer de forma confiável a datação de documento e garantir a sua integridade.

A figura 3.6 mostra o esquema de funcionamento de um PDDE [INS 03].



Figura 3.6: Esquema de funcionamento da Protocoladora Digital de Documentos Eletrônicos

3.8 Conclusão

Neste capítulo foram abordados de forma sucinta diversas técnicas de criptografia que usadas conjuntamente são de fundamental importância para que se possa garantir a validade jurídica de documentos eletrônicos, assunto que será abordado no próximo capítulo.

Capítulo 4

Documento Eletrônico

4.1 Introdução

Este capítulo aborda as definições de documento eletrônico e sua validade jurídica.

4.2 Definição

Para se definir documento eletrônico é necessário primeiramente entender o conceito de documento.

Diversos autores tem sua definição de documento:

Chiovenda [CHI 69] : *”documento, em sentido amplo, é toda representação material destinada a reproduzir determinada manifestação do pensamento, como uma voz fixada duradouramente.”*

José Frederico Marques [MAR 74] : *” documento é a prova histórica real consistente na representação física de um fato. O elemento de convicção decorre, assim, na prova documental , da representação exterior e concreta do factum probandum em alguma coisa.”*

Moacyr Amaral dos Santos [SAN 97] : *”é a coisa representativa de um fato e destinada a fixá-lo de modo permanente e idôneo, reproduzindo-o em juízo.”*

Pontes de Miranda [dM 74] :”o documento, como meio de prova, é toda coisa em que se expressa por meio de sinais, o pensamento.”

Arruda Alvim [ALV 97] : ”prova real (do latim res, rei), dado que todo documento é uma coisa.”

Tendo como base essas e outras definições pode-se dizer de forma mais sistemática que documento é o registro de um fato. Sendo uma de suas características poder ser observado no futuro.

Já no caso de documentos eletrônicos as definições são mais escassas, destacando-se a do Professor Aldemario Araújo Castro [COS 02]: ”documento eletrônico é a representação de um fato concretizada por meio de um computador e armazenado em formato específico (organização singular de bits e bytes), capaz de ser traduzido ou apreendido pelos sentidos mediante o emprego de programa (software) apropriado.”

4.3 Validade Jurídica de Documentos Eletrônicos

Para que um documento eletrônico possa ter força probante, é necessário que algumas características comuns ao documento tradicional estejam presentes:

- Tenha autoria identificável (autenticidade).
- Não possa ser alterado de modo imperceptível (integridade).
- Deve possuir uma forma confiável de datação (tempestividade).

O uso de criptografia assimétrica e assinatura digital garantem os dois primeiros itens, e a utilização de uma PDDE para datar o documento preenche o terceiro requisito.

4.4 Conclusão

Este capítulo tratou das questões referentes a definição de documento eletrônico e sua validade jurídica.

Capítulo 5

S2Card

5.1 Introdução

Neste capítulo será abordado o modelo atual de assinatura digital como SmartCards, o modelo proposto no projeto S2Card e a sua implementação. Projeto que foi idealizado pela equipe do Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina, e primeiramente apresentado pelo Prof. Ricardo Custódio na Escola Norte de Informática [CUS 02].

5.2 Modelo Atual de Assinatura Digital com SmartCards

Nos modelos tradicionais, o SmartCard tem a função armazenar as chaves públicas e privada e assinar o documento, não fazendo nenhuma inferência sobre o tipo de documento que está recebendo. Dessa forma ele simplesmente responde a uma requisição externa sem ter qualquer poder de decisão. A figura (5.1) abaixo dá um exemplo do funcionamento do sistema atual.

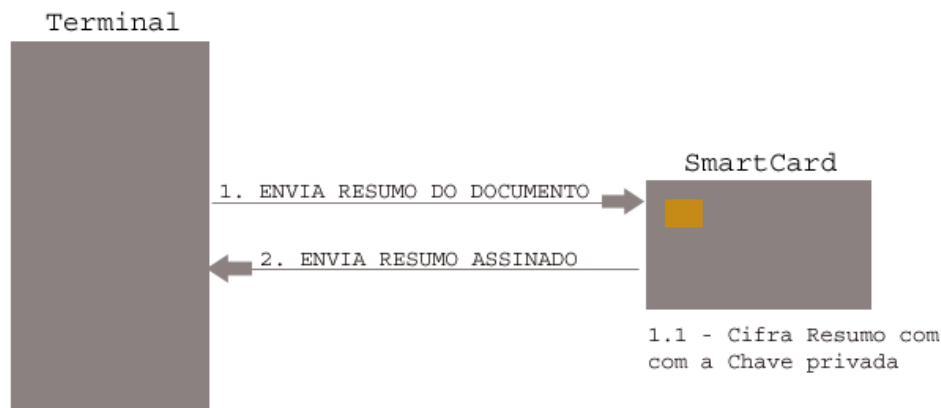


Figura 5.1: Modelo Atual de Assinatura Digital com SmartCards

5.3 Modelo Proposto

Diferente do modelo atual de assinatura digital usando SmartCards, onde o cartão funciona basicamente como portador das chaves pública e privada, no Projeto S2Card, ele passa a desempenhar funções que o tornam verdadeiramente "inteligente", podendo tomar decisões de forma independente.

Além de dar ao cartão autonomia para decidir sobre suas ações, o projeto propõe a criação de um banco de dados para armazenar as assinaturas digitais, possibilitando ao proprietário do cartão um controle maior sobre os documentos por ele assinados.

Outra diferença está no fato de ter-se criado classes de documentos. Estas classes tem como objetivo disciplinar o uso do SmartCard, no sentido de que apenas pessoas autorizadas a assinar determinados tipos de documentos possam fazê-lo.

Por exemplo: No SmartCard de um médico está definido que ele pode assinar um Atestado de Saúde (Classe de Documentos Médicos), porém, se ele tentar usar o seu cartão para assinar uma Escritura (Classe de Documentos Jurídicos), o próprio sistema do cartão irá impedi-lo de efetuar a assinatura. Com isso, cria-se um mecanismo de maior confiabilidade para o processo de assinatura digital, uma vez que o próprio cartão controla as

permissões de assinatura.

Inicialmente estão propostas as seguintes classes:

- Documentos Financeiros
- Documentos Jurídicos
- Documentos Médicos
- Documentos Gerais

Além dessas, está previsto a possibilidade de serem criadas classes específicas para determinados ambientes. Por exemplo:

Uma empresa que deseje usar o sistema pode criar sua própria classe de documentos e ter total autonomia sobre ela.

Outra característica do projeto é o uso de uma função de resumo para o controle de integridade do banco de dados. O SmartCard armazena o resumo dos registros de assinatura do banco de dados, e a cada vez que um registro é inserido um novo resumo é enviado ao cartão. Dessa forma o SmartCard passa a ter controle também sobre o estado do banco de dados. O controle é feito da seguinte forma: No início do processo de assinatura, o cartão compara o resumo que ele possui, com o resumo atual dos registros do banco de dados. Caso sejam iguais, o procedimento de assinatura continua. Do contrário, o SmartCard envia um alerta ao sistema de gerência do banco de dados, para que seja iniciado um processo de auditoria, no sentido de apurar o motivo da diferença entre o resumo atual do banco de dados, e o resumo contido no SmartCard.

Para garantir a tempestividade, que, como foi citado no capítulo anterior, é uma característica obrigatória para que o documento tenha valor legal, é usada uma PDDE (Protocolizadora Digital de Documentos Eletrônicos). Ela irá fornecer a datação de forma confiável à assinatura.

O projeto é dividido em três módulos principais:

- O Applet de controle do SmartCard

- O Sistema do Terminal
- O Sistema de Banco de Dados

Applet de controle do SmartCard - Responsável pelas seguintes funções:

- Verificar a integridade dos registros do banco de dados.
- Verificar se o SmartCard está habilitado a assinar o documento.
- Assinar o documento.
- Verificar assinatura do documento.

O Sistema do Terminal - Responsável pelas seguintes funções:

- Servir como intermediário entre o SmartCard e o banco de dados.
- Solicitar à PDDE a datação confiável para a assinatura
- Obter o resumo do documento que será assinado.
- Apresentar ao usuário o documento assinado.

O Sistema de Banco de Dados - Responsável pelas seguintes funções:

- Armazenar registros das assinaturas digitais
- Calcular o resumo dos registros
- Executar processos automatizados de auditoria e recuperação de erro.

A figura abaixo(Figura 5.2) mostra o processo de assinatura de um documento eletrônico no modelo proposto no projeto S2Card.

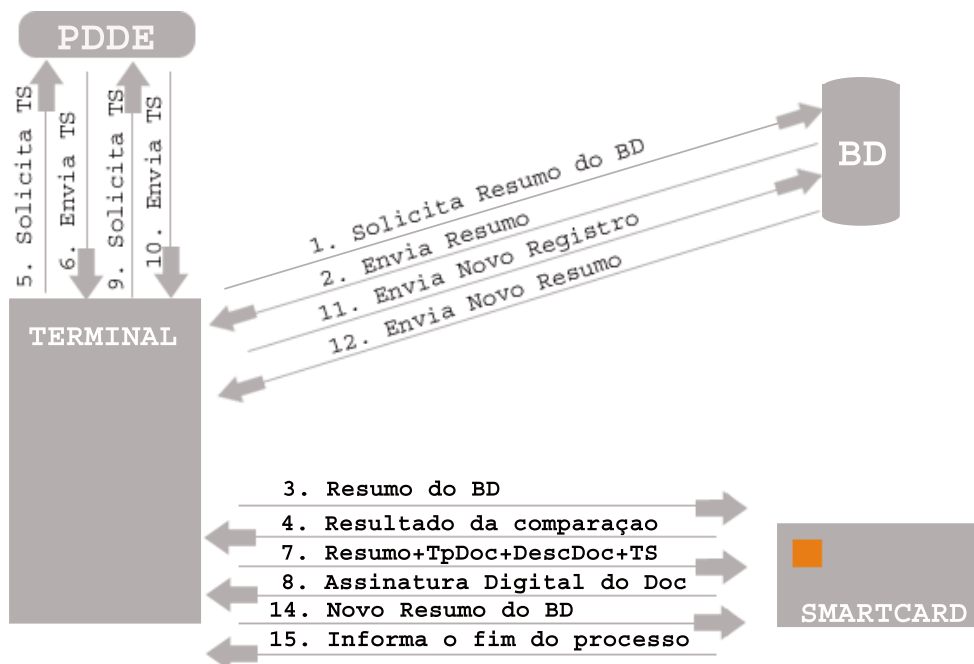


Figura 5.2: Processo de Assinatura no Modelo Proposto

5.4 JavaCard

5.4.1 Definição

JavaCard é um subconjunto da linguagem Java. O padrão JavaCard 2.1, usado no projeto, suporta com exceção do coletor de lixo, todas as características do Java, como pacotes, instanciação dinâmica de objetos, polimorfismo, interfaces e exceções. Apenas tipos complexos como int, long, ou double não estão disponíveis.

5.4.2 Ciclo de Desenvolvimento de um applet para JavaCards

A figura abaixo (Figura 5.3) dá uma visão geral do ciclo de desenvolvimento de um applet para JavaCards.

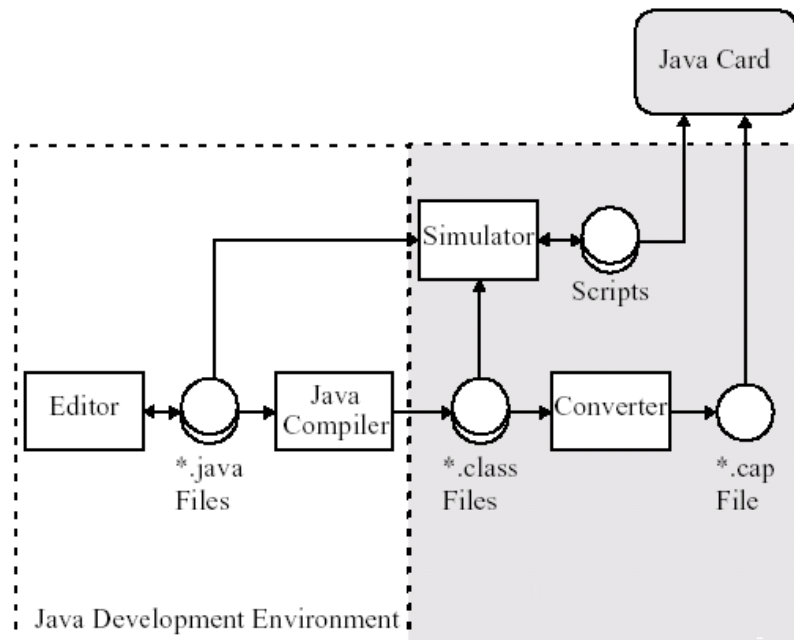


Figura 5.3: Ciclo de Desenvolvimento de um Applet

Os applets podem ser escritos e compilados usando-se qualquer ambiente de desenvolvimento Java.

Uma vez compilados, os arquivos .class, podem ser testados num simulador de JavaCard ou ser convertidos para arquivos .cap e posteriormente carregados no cartão.

5.5 OpenCard framework

O OpenCard framework (OFC) é padrão proposto por consórcio de indústrias, que fornece uma solução para interoperação de sistemas de SmartCards entre diversas plataformas de hardware e software.

Lista de indústrias membros do consórcio:

- 3-G International
- American Express Travel Related Services

- Bull
- First Access
- Gemplus
- Giesecke Devrient
- IBM
- Toshiba Corporation
- TOWITOKO
- Schlumberger
- Siemens
- Sun Microsystems
- UbiQ Inc.
- Visa International
- XAC Automation

5.6 Implementação

5.6.1 Applet de controle do SmartCard

Para o desenvolvimento do applet do SmartCard foram usadas as seguintes ferramentas:

Ambiente de Desenvolvimento : Gel - Native Java IDE versão 086.j, que pode ser encontrado no seguinte endereço: <http://www.gexperts.com>

Conversor e Carregador : Sm@rtCafé Professional versão 1.1 da, gentilmente cedido ao LabSEC pela empresa Giesecke Devrient GmbH, fabricante do programa.

5.6.2 Sistema do Terminal

Para o desenvolvimento do Sistema do Terminal foram usadas as seguintes ferramentas:

Ambiente de Desenvolvimento : Gel - Native Java IDE versão 086.j, que pode ser encontrado no seguinte endereço: <http://www.gexperts.com>

OpenCard framework 1.2

5.7 Funcionamento

O exemplo abaixo mostra um processo executado com sucesso de uma assinatura de documento.

A figura abaixo (Figura 5.4) apresenta a tela inicial do processo de assinatura.

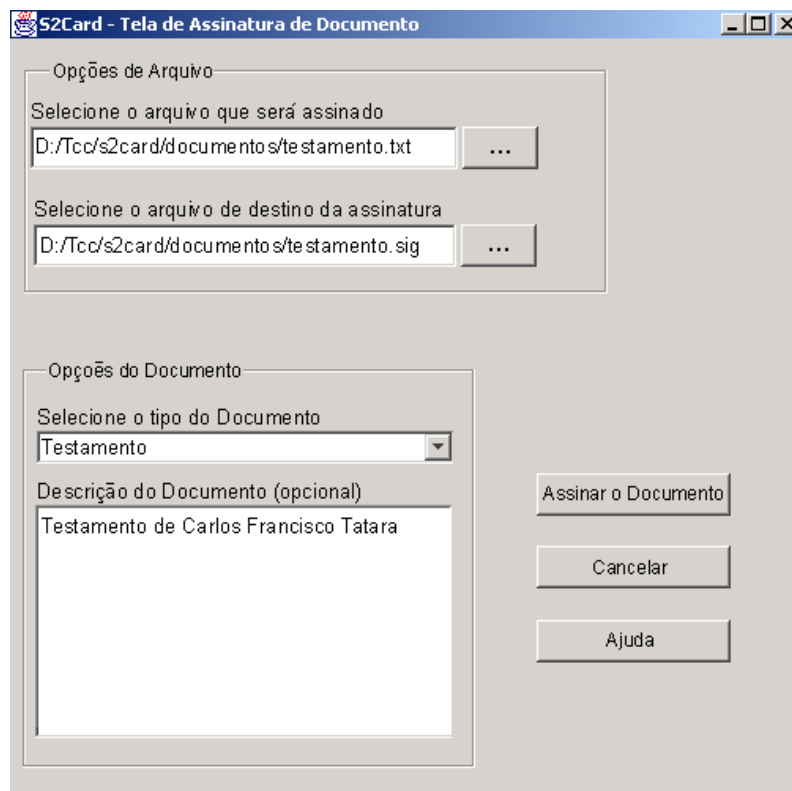


Figura 5.4: Tela inicial de assinatura

Ao clicar no botão "Assinar o Documento", o protocolo apresentado na Figura 5.2 é iniciado.

O terminal solicita a inserção de um SmartCard no leitor (Figura 5.5).

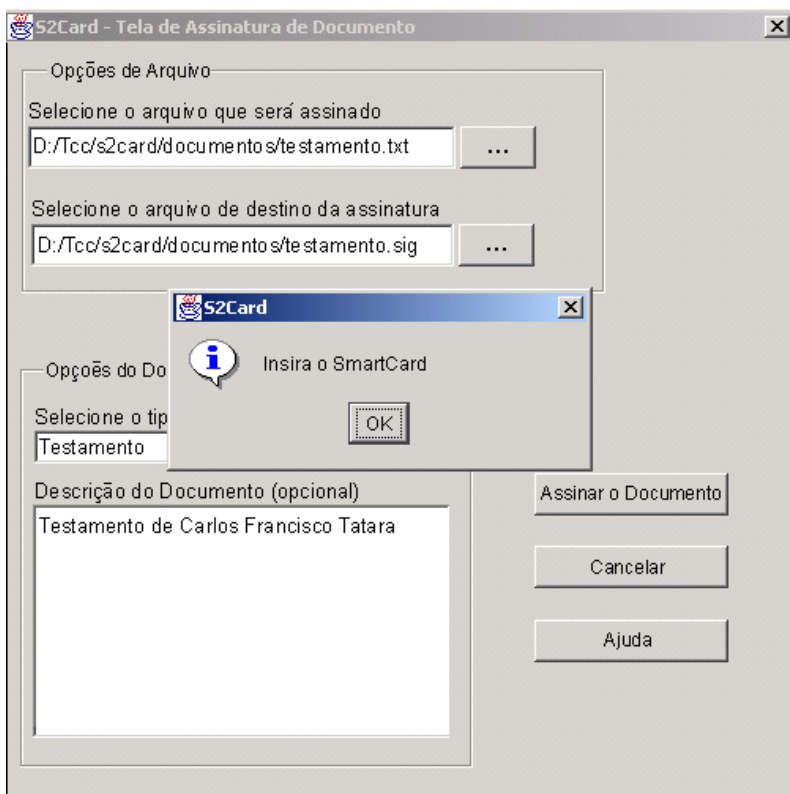


Figura 5.5: Tela de solicitação de inserção do SmartCard

Trecho de código referente a ação de inicialização do JavaCard framework:

```

JOptionPane.showMessageDialog( null,"Insira o
SmartCard","S2Card",JOptionPane.INFORMATION MESSAGE);
try
//Inicializa o framework
SmartCard.start ();
CardRequest cr = new CardRequest ();

```

```
cr.setWaitBehavior (CardRequest.ANYCARD);  
SmartCard sm = SmartCard.waitForCard (cr);
```

A próxima tela solicita (Figura 5.6) que o usuário digite o seu PIN para que o processo de assinatura possa ser iniciado

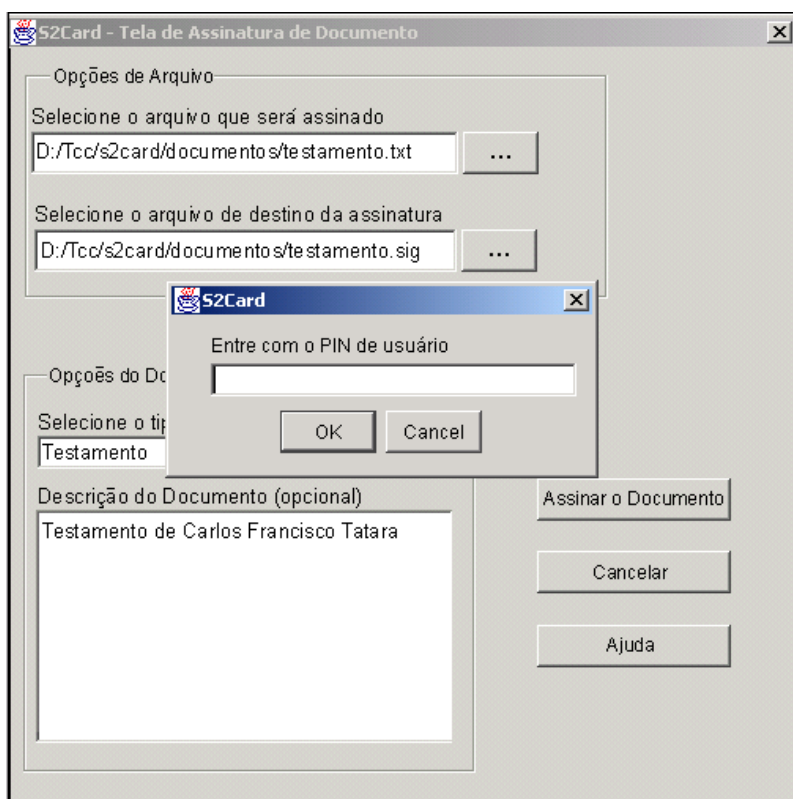


Figura 5.6: Tela de solicitação do PIN do usuário

A tela a seguir (Figura 5.7) é apresentada ao usuário enquanto o processo de assinatura é executado.

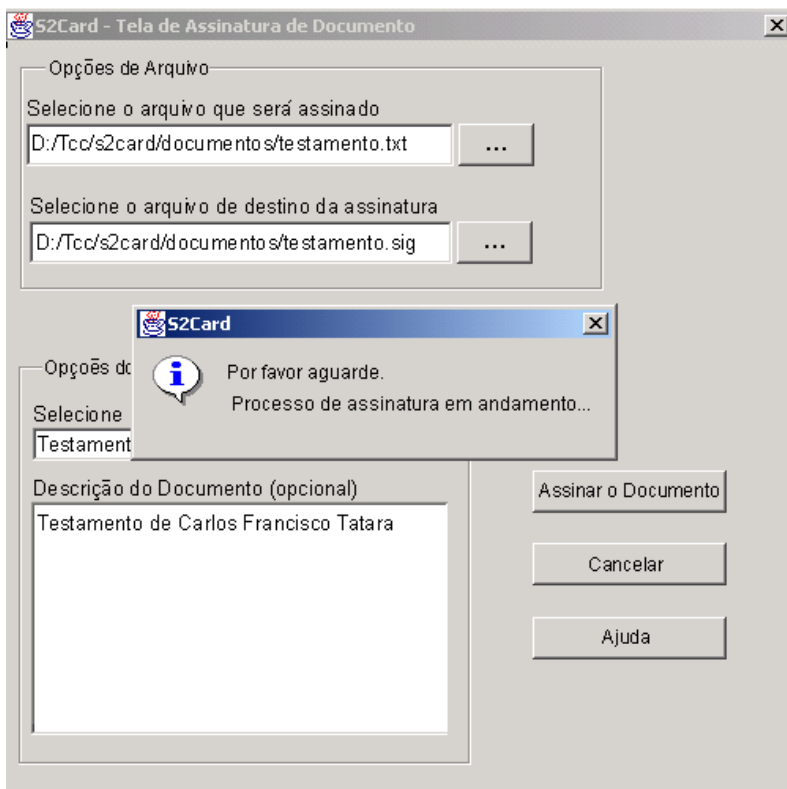


Figura 5.7: Processo de assinatura digital em andamento

Nesse momento a seguinte seqüência de comandos é enviada ao Smart-Card:

Comando que envia o resumo do Banco de Dados para verificação da sua integridade:

```
response = factory.sendAPDU(new CommandAPDU((byte),INTEGRIDADEBD,
(byte)0x0, (byte)0x0, hashbd, (byte)0));
```

Comando que envia o tipo de documento para verificar se o cartão pode assiná-lo:

```
response = factory.sendAPDU(new CommandAPDU((byte),TIPODOC,
(byte)0x0, (byte)0x0, tipodoc, (byte)0));
```

Comando que envia a descrição do documento:

```
response = factory.sendAPDU(new CommandAPDU((byte),DESCDOC,
(byte)0x0, (byte)0x0, descdoc, (byte)0));
```

Comando que envia o resumo do documento para o cartão cifrar: `response = factory.sendAPDU(new CommandAPDU((byte),ASSINAR,(byte)0x0, (byte)0x0, hashbd, (byte)0));`

Comando que envia o novo resumo do banco de dados para substituir o antigo que estava no cartão:
`response = factory.sendAPDU(new CommandAPDU((byte),NOVOHASH,(byte)0x0,(byte)0x0, novoHashbd,(byte)0));`

5.8 Conclusão

Este capítulo discutiu o modelo atual de assinatura digital com SmartCards, e o modelo proposto no Projeto S2Card. Também abordou informações sobre a implementação do projeto.

Capítulo 6

Conclusão

Este trabalho descreveu a proposta de implementação de um novo modelo de assinatura digital utilizando SmartCards.

Fez-se uma pesquisa sobre a tecnologia de cartões, abordou-se temas sobre criptografia relevantes ao projeto, e discutiu-se sobre documentos eletrônicos e sua validade jurídica.

Também foi abordado o modelo atual de assinatura digital com SmartCards, onde o cartão funciona basicamente com portador das chaves pública e privada.

No modelo proposto, o processo ganha maior confiabilidade devido ao fato de se restringir a assinatura de determinados tipos documentos apenas àquelas pessoas que de fato tem competência para realizá-la.

Outro ponto que aumenta a transparência do processo é o fato de se manter um registro de todas as assinaturas executas pelo cartão, facilitando desta forma qualquer processo de auditoria ou qualquer tipo de disputa jurídica onde seja questionada a autenticidade da assinatura.

Referências Bibliográficas

- [ALV 97] ALVIM, A. **Manual de Direito Processual Civil**. 6^l. ed. São Paulo: RT, 1997.
- [AM 96] ALFRED MENEZES, P. VAN OORSCHOT, S. V. **Handbook of Applied Cryptography**. CRC Press, 1996.
- [CHI 69] CHIOVENDA, G. **Instituições de Direito Processual Civil. Trad. Da 2 Edição Italiana Por J. Guimarães Menegale**. 3. ed. São Paulo: Saraiva, 1969.
- [COS 02] COSTA, A. A. **Instituto Brasileiro de Direito Eletrônico**. Disponível em <<http://www.idbe.org.br/doceletronico.doc>>. Acesso em: novembro de 2002.
- [CUS 02] CUSTÓDIO, R. F. **Tecnologias Para a Segurança Da Informação: Infra-Estrutura de Chaves Públicas**. Escola de Informática Norte.
- [Dep 93] Department of Commerce. **Secure Hash Standard**, Maio, 1993. Federal information processing standards publication 180.
- [DIF 76] DIFFIE, W.; HELLMAN, M. **New Direction in Criptography**.
- [dM 74] DE MIRANDA, F. C. P. **Comentários as Código de Processo Civil**. 3. ed. São Paulo: Saraiva, 1974.
- [INS 03] INSTITUCIONAL, S. **PDDE - Protocolizadora**.
<https://trtapl.trt12.gov.br/scripts/peticao/msg/pdde-detalhado.asp>.
- [KOC 98] KOCHER, P. **Differential Power Analysis**. Disponível em <<http://www.cryptography.com/dpa>>. Technical Report.
- [MAR 74] MARQUES, J. F. **Manual de Direito Processual Civil**. São Paulo: Saraiva, 1974.
- [PAS 01] PASQUAL, E. S. **IDDE - Uma Infra-Estrutura Para Datação de Documentos Eletrônicos**. Curso de Pós-Graduação em Ciência da Computação - Universidade Federal de Santa Catarina, 2001. 102 p. Dissertação.
- [RIV 92] RIVERST, R. **The Md5 Message Digest Algorithm**. Network Working Group. Request for comments: 1321.

- [RR 76] RON RIVERST, A. S.; ADLEMAN, L. **A Method for Obtaining Digital Signatures and Public Key Cryptosystems**. Communications of the ACM.
- [SAN 97] SANTOS, M. A. D. **Primeiras Linhas de Direito Processual Civil**. 18 (revista, atualizada e ampliada por Aricê Moacyr Amaral dos Santos). ed. Saraiva, 1997.
- [SCH 96] SCHNEIER, B. **Applied Cryptography**. 2. ed. New York: John WileySons, 1996.
- [STA 98] STALLINGS, W. **Cryptography and Network Security: Principles and Practice**. 2. ed. Upper Saddle River, New Jersey 07458: Prentice Hall, 1998.
- [Thi 96] Third International Workshop on Fast Software Encryption. **RIPEMD-160: A Strengthened Version of RIPEMD**. Springer-Verlag, 1996.

Apêndice A

Anexos