CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
MESTRADO EM TECNOLOGIA

MARIA DE FÁTIMA BERNARDI

PROPOSTA DE UM MODELO DE AUTENTICAÇÃO SEGURA PARA ACESSO A SITES DE ENSINO À DISTÂNCIA UTILIZANDO BIOMETRIA E CARTÕES INTELIGENTES

SÃO PAULO

JUNHO, 2007

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA

MARIA DE FÁTIMA BERNARDI

PROPOSTA DE UM MODELO DE AUTENTICAÇÃO SEGURA PARA ACESSO A SITES DE ENSINO À DISTÂNCIA UTILIZANDO BIOMETRIA E CARTÕES INTELIGENTES

SÃO PAULO

JUNHO, 2007

MARIA DE FÁTIMA BERNARDI

PROPOSTA DE UM MODELO DE AUTENTICAÇÃO SEGURA PARA ACESSO A SITES DE ENSINO À DISTÂNCIA UTILIZANDO BIOMETRIA E CARTÕES INTELIGENTES

Dissertação apresentada como exigência parcial para obtenção do Título de Mestre em Tecnologia no Centro Estadual de Educação Tecnológica Paula Souza, no Programa de Mestrado em Tecnologia: Gestão Desenvolvimento e Formação, sob orientação do Dr. Prof. Maurício Amaral de Almeida.

SÃO PAULO

JUNHO, 2007

B523p Bernardi, Maria de Fátima

Proposta de um modelo de autenticação segura para acesso a sites de ensino a distância utilizando biometria e cartões inteligentes.– São Paulo : CEETEPS, 2005.

118 f.

Dissertação (Mestrado) – Centro Estadual de Educação Tecnológica Paula Souza, 2004.

1.Educação a distância. 2. Cartões inteligentes. 3. Bio metria. I. Título.

CDU 37.018.43

MARIA DE FÁTIMA BERNARDI

PROPOSTA DE UM MODELO DE AUTENTICAÇÃO SEGURA PARA ACESSO A SITES DE ENSINO À DISTÂNCIA UTILIZANDO BIOMETRIA E CARTÕES INTELIGENTES

_____

PROF. DR. MAURÍCIO AMARAL DE ALMEIDA

_____

PROFa. DRA. MARIA EMILIA GOMES SOBRAL

_____

PROFa. DRA. HELENA GEMIGNANI PETEROSSI

São Paulo, 15 de junho de 2007.

Dedicatória

À pessoa mais importante da minha vida: minha mãe!

AGRADECIMENTOS

Agradecer por algo é um modo de demonstrar não somente gratidão, mas também de dizer o quanto este algo é ou foi importante para nós. Assim, gostaria de deixar registrado meu sincero voto de agradecimento a todas as pessoas que participaram, direta ou indiretamente, na confecção deste trabalho. E em especial a pessoa que me incentivou a entrar nesta jornada de 2 anos de estudos, pesquisas e descobrimento de novas coisas, inclusive pessoais. Obrigada!

RESUMO

BERNARDI, M. F. **Proposta de um modelo de autenticação segura para acesso a sites de ensino à distância utilizando biometria e cartões inteligentes.** 2004. 99 f. Dissertação (Mestrado em Tecnologia) – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2007.

Este trabalho foi desenvolvido com a finalidade de buscar as alternativas de soluções usando cartões inteligentes e métodos biométricos existentes no mercado e propor uma solução da utilização destas duas tecnologias para garantir a autenticação usuários a sites de ensino à distância.

As tecnologias de cartões inteligentes e os métodos biométricos desenvolvidas até hoje foram verificadas para se chegar a um desenho final de solução que pudesse ser implementado posteriormente. O intuito deste trabalho não era o desenvolvimento final de um sistema e sim, propor uma solução que pudesse ser implementada.

O foco principal do trabalho foi estudar as tecnologias e encontrar a melhor solução para a resolução do problema proposto.

A partir disto, a solução foi desenhada baseando-se nos estudos e pesquisas realizados e utilizando o resultado destas pesquisas para que pudesse chegar a uma solução final.

Palavras-Chave: Smart Cards, Métodos biométricos, Cartões Inteligentes, Biometria, Autenticação de usuários.

ABSTRACT

BERNARDI, M. F. **The use of the smart cards and biometrics methods for user authentication for distance learning sites.** 2004. 99 f. Dissertação (Mestrado em Tecnologia) – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2007.

This work was developed with finality to find the solution alternatives using smart cards and biometrics methods existents in the market and to propose a solution to use these both technologies to provide the user authentication for distance learning sites.

The Technologies of the smart cards and biometrics methods developed until now were verified to get a final solution design that could to be implemented later. The intuit of this work wasn't the final development of the system, but, to propose a solution that could to be implemented.

The main focus of this work was study the technologies and find the best solution for the resolution of the propose problem.

After this, the solution was designing with base in the studies and researches realized and using the result of these researches to get the final solution.

Keywords: Smart Cards, Biometrics methods, Biometry, User authentication.

Lista de Figuras

Figura 1 – Tela de entrada de sistema de EAD – Fonte: UFMG 21
Figura 2 – Tela de entrada de site de EAD 22
Figura 3 – Estrutura da família de cartões inteligentes 27
Figura 4 – Arquitetura típica de um cartão memória com segurança lógica 27
Figura 5 – Arquitetura típica de um cartão microprocessado 29
Figura 6 – Definição de dimensões do formato ID-1 31
Figura 7 – O formato ID-1 31
Figura 8 – Localização dos contatos em relação ao corpo do cartão 32
Figura 9 – Tamanho mínimo dos contatos de acordo com ISO 7816-2 33
Figura 10 – Placa de silício (Wafer) e rolo de chip 35
Figura 11 – Microchip pronto 35
Figura 12 – Processo de fabricação dos módulos 36
Figura 13 – Instalação do módulo do chip no corpo do cartão 38
Figura 14 – Processo do uso de um sistema biométrico 43
Figura 15 – Impressão digital mostrando os pontos de verificação
e as rugas de bifurcação e final 47
Figura 16 – Diferença entre Linha rígida e linha de fluxo 47
Figura 17 – Comparação entre impressões digitais 48
Figura 18 – Etapas do reconhecimento facial 50
Figura 19 – Anatomia da produção da fala 51
Figura 20 – Processo de scaning para reconhecimento da íris 53
Figura 21 – Posição circular da íris 54
Figura 22 – Otimizando a imagem 54
Figura 23 – Identificação dos vasos sanguíneos e mapeamento completo 56
Figura 24 – Retinas de irmãos gêmeos 56
Figura 25 – Funções da Infra-estrutura de Chaves Públicas para Certificação
Digital 60

Figura 27 – Tela de entrada de usuário 65
Figura 28 – Estrutura completa do cartão 67
Figura 29 – Estrutura do campo SENHA 68
Figura 30 – Estrutura do campo NOME 69
Figura 31 – Estrutura do campo FINGER 70
Figura 32 – Estrutura do campo CERTIFICADO 71
Figura 33 – Estrutura do processo físico 75

Índice de Tabelas

Tabela 1 – Comparação de métodos biométricos 57

SUMÁRIO

1. INTRODUÇÃO 14

2. FUNDAMENTAÇÃO TEÓRICA 18

2.1 ENSINO À DISTÂNCIA 18
2.2 CARTÕES INTELIGENTES 25
2.3 BIOMETRIA 40
2.4 CERTIFICAÇÃO DIGITAL 57

3. DESENVOLVIMENTO 62

3.1 MODELO PROPOSTO 65
3.2 DESCRIÇÃO DO SISTEMA 65
3.3 PROCESSO FÍSICO 74

4. CONCLUSÃO 77

REFERÊNCIAS BIBLIOGRÁFICAS 79

BIBLIOGRAFIA BÁSICA 79
BIBLIOGRAFIA COMPLEMENTAR 82

GLOSSÁRIO 84

ANEXOS 88

ANEXO I - DIAGRAMA DE CASO DE USO 89
ANEXO II - DESCRIÇÃO DE CASO DE USO 90
ANEXO III - DIAGRAMA DE CLASSE 91
ANEXO IV - DIAGRAMA DE SEQÜÊNCIA 92
ANEXO V - DESCRIÇÃO DA FUNÇÃO PRINCIPAL 93
ANEXO VI - DESCRIÇÃO DA FUNÇÃO CONSULTA_USUARIO() 95
ANEXO VII - DESCRIÇÃO DA FUNÇÃO VERIFICA_CERTIFICADO() 96
ANEXO VIII - DESCRIÇÃO DA FUNÇÃO VERIFICA_REG_CARTAO() 97
ANEXO IX - DESCRIÇÃO DA FUNÇÃO COMPARA_TEMPLATE() 98

1. INTRODUÇÃO

O avanço da tecnologia e dos sistemas computacionais nos trouxe certa dependência, pois quase todos os sistemas que utilizamos hoje, ou que necessitamos acessar são baseados em computadores, sejam eles em nossa casa ou trabalho.

Muitas vezes necessitamos acessar esses sistemas utilizando informações que possuímos para que possamos nos autenticar neles mesmo. Ora utilizamos nosso nome ou nossa senha. Porém, na maioria das vezes isto não resulta em grande segurança para o sistema ou para nós mesmos.

Assim, o conceito de autenticação engloba a verificação da identidade do usuário, o conhecimento dos dados e o objeto de autenticação. Desta forma, podemos resumir este conceito utilizando os três mecanismos de verificação da identidade de um usuário. Este conceito engloba as seguintes categorias: ”Quem você é”, “O que você sabe” e “O que você tem”. (LIU; SILVERMAN, 2003).

Com estas três categorias podemos proporcionar uma segurança maior em qualquer sistema computacional utilizando a junção dos processos de identificação, com programas e equipamentos apropriados para isto.

O objetivo da utilização de autenticações é de garantir a segurança no acesso aos sistemas, pois mecanismos de autenticação são críticos para a segurança de qualquer sistema computacional (NIST, 2004).

Nos dias de hoje, vários processos de autenticação são utilizados em diversos ambientes, principalmente em ambientes comerciais. Porém, a utilização de processos de autenticação em ambientes de ensino à distância não está sendo muito utilizado.

A grande dúvida é saber se a pessoa que está acessando ao sistema é realmente a pessoa que deveria acessá-lo. Em levantamento realizado com alguns

sites de ensino à distância (UFMG, 2004); (CEDERJ, 2004) foi verificado que alguns deles não utilizam nenhum sistema de identificação ou autenticação do usuário e outros utilizam apenas a combinação do nome do aluno (*login*) e uma senha. Esta combinação simples pode acarretar falha de segurança no processo de autenticação do mesmo, pois caso outro usuário souber estas informações, pode acessar o sistema e obter suas informações indevidamente.

Assim, o que podemos concluir é que sistemas baseados em senhas são fracos, pois existem vários métodos disponíveis, inclusive na própria Internet, para quebrar senhas das mais simples até as mais complexas.

Desta maneira, a contextualização do problema é como garantir a autenticação de um usuário a um site de EAD.

Para solucionar este problema e garantir esta autenticação segura dos usuários, este trabalho realizará uma pesquisa dos métodos de segurança, sugerindo meios de autenticação segura para o acesso do usuário ao site de EAD.

O objetivo deste trabalho é de desenhar uma solução para que se possa ter segurança no acesso de usuários aos sites de EAD, bem como, mostrar como desenvolver soluções para resolver um determinado problema, fazendo com que a tecnologia possa ser utilizada em conjunto para tal finalidade.

Não faz parte deste trabalho, o desenvolvimento de uma aplicação final para o acesso de usuários a sites de EAD e o levantamento de custos dos equipamentos estudados.

A hipótese deste trabalho é verificar se a solução proposta realmente terá resultados satisfatórios e atingirá o objetivo desejado.

Para o levantamento das informações utilizadas neste trabalho foi utilizado o método qualitativo, onde foram realizadas diversas consultas a diferentes fornecedores de cartões inteligentes e equipamentos biométricos. O foco destas consultas não foi se limitar aos fornecedores, e sim, achar uma solução que pudesse

atender as necessidades do problema. Todavia, para complementar o trabalho, foi necessário à utilização de um determinado cartão e um determinado equipamento de biometria. Porém, não é necessário que se utilize somente este produto, pois atendendo a especificação do mesmo, qualquer produto similar poderá ser utilizado.

Assim, este trabalho foi desenvolvido subdivido em três partes.

A primeira parte apresenta a fundamentação teórica, subdividida em quatro itens. O primeiro item faz um breve resumo sobre o ensino à distância, fazendo um histórico da sua criação, seu funcionamento, as necessidades e mostrando uma pesquisa realizada com alguns grupos de EAD.

O segundo item descreve os cartões inteligentes, fazendo um histórico sobre sua criação, desenvolvimento e o atual estado da arte, incluindo um resumo tecnológico. São descritos também, os padrões, especificações e formatos que estes cartões devem seguir e utilizar. Uma explicação de como funciona um cartão com contato e quais os métodos de sua produção também estão relatados.

No terceiro item foi escrita a parte da biometria, fazendo um histórico sobre sua criação, desenvolvimento e o atual estado da arte. São descritos também, os métodos e padrões biométricos e alguns métodos biométricos mais utilizados atualmente.

No quarto item foi realizada uma descrição sobre o que é e como funciona a certificação digital.

A segunda parte do trabalho descreve o desenvolvimento do sistema. Esta parte foi subdividida em três itens. O primeiro item mostra o modelo proposto utilizando técnicas de UML. O segundo item faz a descrição propriamente dita do sistema, com as definições de funcionamento do cartão e as funções que são necessárias para que o sistema funcione corretamente. O terceiro item descreve o processo físico do sistema, sendo relatadas as características físicas de equipamento que são necessárias para o seu perfeito funcionamento.

Na terceira parte do trabalho, a conclusão do trabalho, relatando os resultados finais, as vantagens e desvantagens da proposta sugerida e mostrando o que poderá ser desenvolvido em próximas etapas.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 Ensino à Distância

2.1.1 Histórico

Educação à distância já vem sendo abordada há muito tempo. Podemos começar a tratar este assunto pela origem da palavra “tele”, visto que tele-ensino também pode ser designado como ensino à distância. A palavra “tele” tem sua origem no grego, e seu significado é “ao longe”, o que podemos associar com “à distância”.

Segundo pesquisas realizadas, a origem da educação à distância vem de épocas remotas, ou seja, desde as cartas de Platão e as epístolas de São Paulo e do Novo Testamento, pois eram destinadas a comunidades inteiras e possuíam um grande caráter didático. (ANDRADE, 1997).

Porém, o grande avanço da EAD (Ensino à Distância) deu-se no século XV com a invenção da imprensa por *Johannes Guttemberg*. Esta invenção possibilitou a composição de palavras com caracteres móveis e a confecção de livros copiados com maior rapidez do que os métodos anteriores. Com esta criação, tornou-se possível ler livros sem ter a necessidade de mestres que os lessem para seus alunos.

Há registros de experiências de educação por correspondência iniciadas no final do século 19 na Suécia, Inglaterra, Alemanha e Estados Unidos. No Brasil consta o inicio de EAD em 1904 com a implantação das “Escolas Internacionais”. (ALVES, 2004).

Na atualidade, o surgimento do rádio, da televisão e o uso do computador como meio de comunicação deram nova dinâmica ao ensino à distância. Cada um

desses meios introduziu um novo elemento ao EAD:

- O rádio permitiu que o som (em especial a voz humana) fosse levado a localidades remotas. Assim, a parte sonora de uma aula pode, com o rádio, ser colocada remotamente. O rádio está disponível desde o início da década de 20, quando a KDKA (prefixo de rádio) de Pittsburgh, PA, tornou-se a primeira emissora de rádio comercial a operar.

- A televisão permitiu que a imagem fosse, junto com o som, levada às localidades remotas. Assim, agora uma aula quase inteira, englobando todos os seus componentes audiovisuais, pode ser aplicada remotamente. A televisão comercial está disponível desde o final da década de 40.

- O computador permitiu que o texto fosse enviado com facilidade a localidades remotas ou fosse buscado com facilidade em localidades remotas. O correio eletrônico permitiu que as pessoas se comunicassem com extrema rapidez. Mais recentemente, o aparecimento de "*chats*" ou "bate-papos" permitiu a comunicação em tempo real entre várias pessoas. E, mais importante, a Internet permitiu não só que fosse agilizado o processo de acesso a documentos textuais, mas hoje abrange gráficos, fotografias, sons e vídeo. Além de permitir o acesso a todo esse material fosse feito de forma não-linear e interativa, usando a tecnologia de hipertexto. O primeiro computador foi mostrado ao mundo em 1946, mas foi só depois do surgimento e do uso maciço de microcomputadores (que apareceram no final de 1977) que os computadores começaram a serem vistos como tecnologia educacional. A Internet, embora tenha sido criada em 1969, só explodiu no mercado mesmo nos últimos dez anos, quando foi aberta para uso comercial (pois antes servia apenas a comunidade acadêmica).

- A convergência de todas essas tecnologias em um só mega-meio de comunicação, centrado no computador, e, portanto, interativo, permitiu a realização de conferências eletrônicas envolvendo componentes audiovisuais e textuais. (CHAVES, 1999).

Como definição, podemos dizer que EAD é a “modalidade de educação em que as atividades de ensino-aprendizagem são desenvolvidas majoritariamente sem que alunos e professores estejam presentes no mesmo lugar à mesma hora”. (ABED, 2004).

2.1.2 Funcionamento

Para que um programa de EAD tenha sucesso, podemos enumerar três elementos de fundamental importância:

- Projeto: métodos de instrução tradicional não podem ser utilizados no EAD. Novos projetos de aprendizado devem ser desenvolvidos para tirar proveito dos benefícios trazidos pelas novas tecnologias;
- Tecnologia: a forma de utilização da tecnologia pode ser o motivo do sucesso ou do fracasso;
- Suporte: fornecer suporte aos usuários pode incentivar novos usuários a desenvolver ou expandir caminhos eficientes e efetivos no que se refere a métodos de EAD. (UFRS, 1998).

Em pesquisa realizada no Brasil pela revista “Pequenas Empresas & Grandes Negócios”, foi verificado que a atividade de EAD cresce cerca de 35% ao ano estimulada pela demanda das grandes empresas, que passaram a adotar o treinamento on-line como forma de atualizar seus funcionários, sendo que as universidades também estão utilizando EAD e algumas oferecem 20% de seus cursos de forma remota e existe a perspectiva de que essa porcentagem suba para 50%. A Secretaria de Educação a Distância já deixou clara a intenção do governo federal de investir em EAD, levando o método até para as escolas públicas. (PE&GN, 2004).

Porém, nas consultas realizadas em diversos sites de EAD e em matérias sobre o assunto, não foi verificado nenhum processo ou quesito referente à segurança de acesso dos usuários aos respectivos sites. Somente alguns dos *sites*

utilizam o processo de identificação do aluno através da utilização de *login* e senha.

Como exemplo, podemos citar o *site* dos cursos Ensino à Distância oferecidos pela Universidade Federal de Minas Gerais (UFMG), que após a inscrição do aluno, utiliza uma página de entrada (Figura 1) onde solicita os dados do usuário e senha.

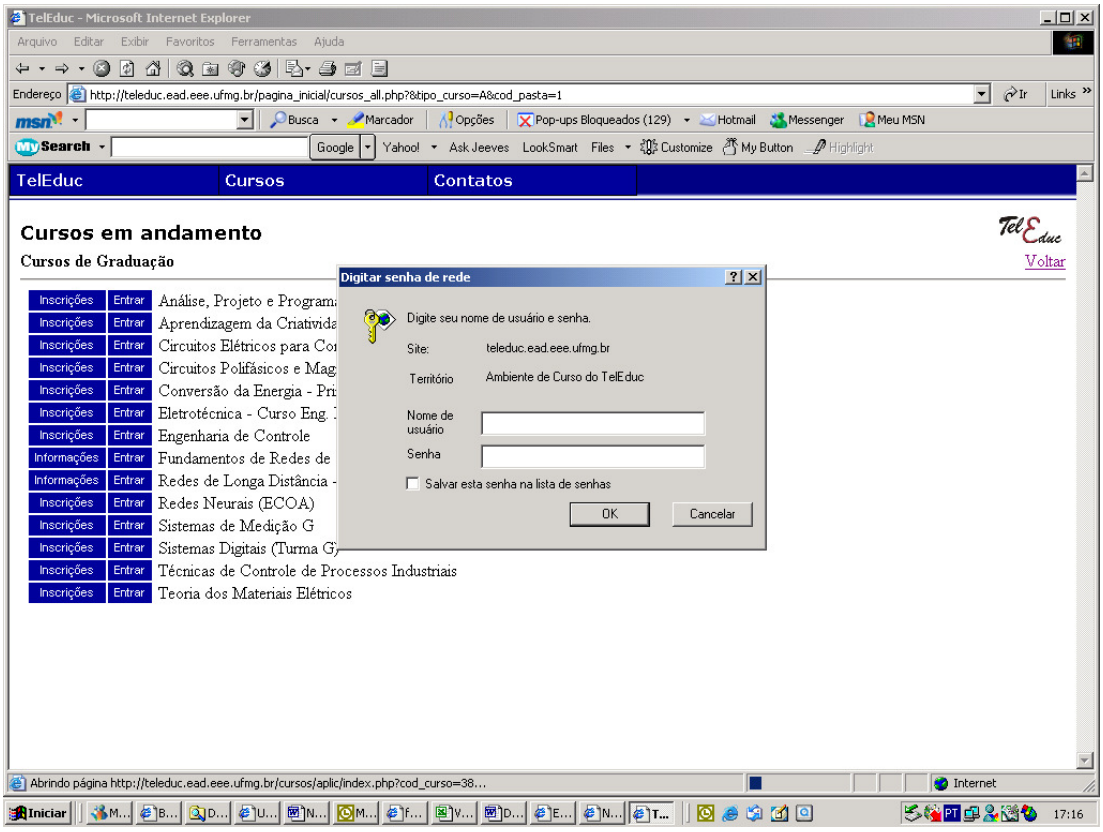


Figura 1: Tela de entrada de sistema de EAD
Fonte: (UFMG, 2004)

Em outro site de EAD para o *Curso de Licenciatura em Biologia* oferecido pelo CEDERJ, também foi verificado que o acesso aos alunos cadastrados dá-se através da informação do Usuário e Senha (Figura 2).

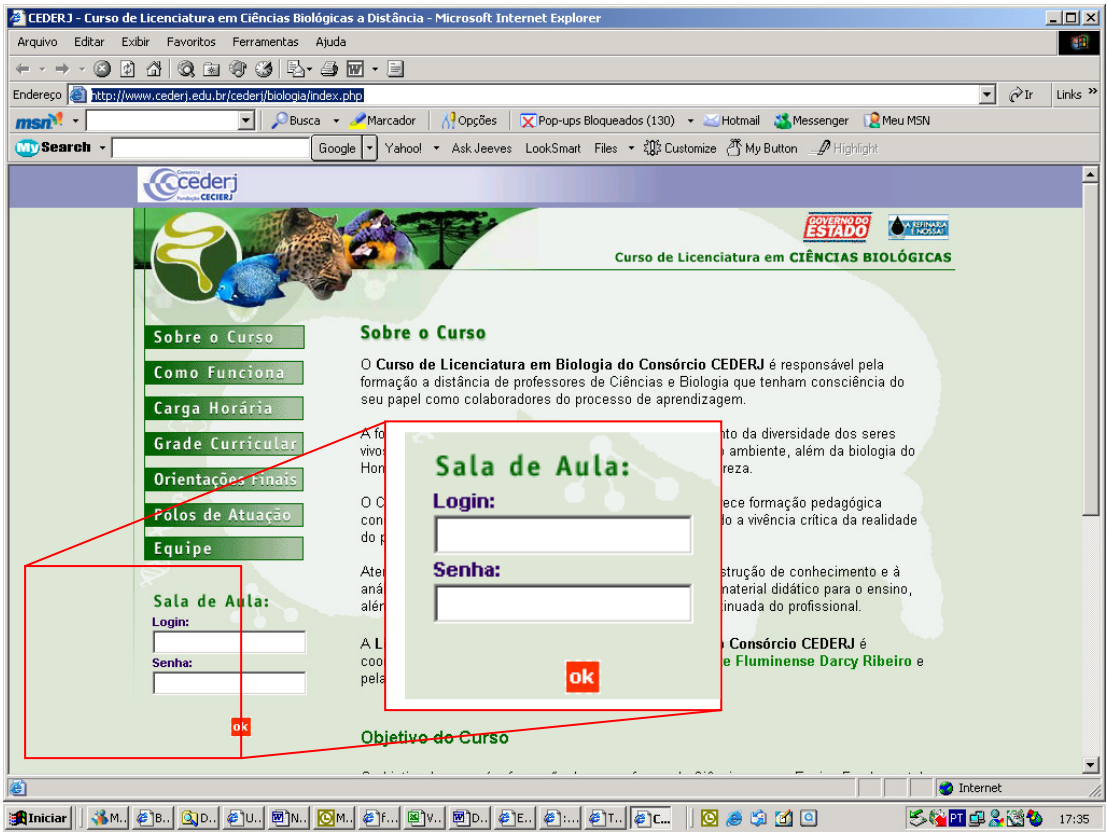


Figura 2: Tela de entrada de site de EAD.

Fonte: (CEDERJ, 2004)

Em nenhum dos *sites* visitados foi verificado um interesse maior ou uma alusão da necessidade de utilização de outros meios de acesso além do tradicional “Usuário / Senha”.

2.1.3 Necessidades de EAD

Para verificar a real necessidade de segurança no processo de autenticação de um usuário a um *site* de EAD, foi elaborado um questionário e enviado para alguns grupos de pesquisa para que os mesmos pudessem relatar suas experiências.

Entre os grupos consultados estão: o GEADI – Grupo de Ensino à Distância do Centro Paula Souza – SP e a ABED – Associação Brasileira de Ensino à Distância.

Questionário enviado por email para os grupos acima citados em 12 de julho de 2004. Esta pesquisa foi realizada com base das nove perguntas descritas abaixo:

Pergunta 1: No processo de EAD, quais as maiores dificuldades de verificação da existência do aluno, ou seja, como vocês têm a certeza que o aluno inscrito é realmente o aluno que está assistindo às aulas e fazendo as provas?

Resposta: Os grupos pesquisados informaram que para o sistema ter credibilidade, pelo menos até agora, é necessário que todas as avaliações sejam presenciais.

Pergunta 2: Como vocês vêm um processo de autenticação do aluno no momento em que o mesmo acessa ao *site* de EAD e no decorrer de seu aprendizado?

Resposta: Os grupos responderam que este processo é fundamental, pois estariam eliminando a presença do aluno no momento das avaliações.

Pergunta 3: Existe realmente a necessidade de certificar se é o aluno inscrito

que está acessando o *site* de EAD?

Resposta: Os grupos responderam que existe esta necessidade, principalmente nos cursos onde a certificação tenha validade nacional e / ou internacional.

Pergunta 4: Atualmente qual o processo que vocês utilizam em seus cursos de EAD para autenticação do aluno?

Resposta: A ABED respondeu que os seus associados utilizam somente o cadastro de usuário e senha. O GEADI informou não utilizar nenhum processo de autenticação por falta de estrutura.

Pergunta 5: Se fosse proposto um processo de autenticação segura que pudesse aumentar a garantia da presença do aluno inscrito ao *site* de EAD, isto ajudaria no trabalho de vocês?

Resposta: Ambos os grupos responderam que sim.

Pergunta 6: Vocês acham que seria necessária a autenticação segura do aluno em qualquer *site* de EAD ou seria interessante somente nos cursos onde o curso é pago?

Resposta: Neste caso houve controvérsia, a ABED informou não ser de grande importância utilizar a autenticação em cursos gratuitos. Já o GEADI informou que seria importante utilizar em qualquer curso de EAD.

Pergunta 7: Quais as vantagens e desvantagens que vocês vêm em um processo de autenticação seguro do aluno ao site de EAD?

Resposta: As repostas foram positivas devido a verem somente vantagens neste processo, pois com um sistema de autenticação se teria maior certeza de que o aluno inscrito está realmente participando do curso.

Pergunta 8: Vocês poderiam me informar se, em suas pesquisas, já se depararam com algum *site* de EAD que já utiliza as tecnologias de cartões inteligentes e biometria para a autenticação de usuários?

Resposta: As repostas foram que desconhecem esta utilização e que no máximo, o acesso ao sistema é realizado através de *login* de usuário e senha.

Pergunta 9: Se sim, vocês poderiam me repassar estas informações?

Resposta: Não houve respostas.

2.2 Cartões Inteligentes

2.2.1 Histórico

A história dos cartões inteligentes confunde-se com a própria história dos cartões de plástico. A proliferação de cartões de plástico começou nos EUA no início dos anos 50. O baixo preço do material sintético de PVC possibilitou a produção de um cartão robusto, elástico, muito mais conveniente para os dias atuais que os seus antecessores de papel ou de papelão. (RANKL; EFFING, 2000).

Com o progresso da microeletrônica nos anos 70, tornou-se possível integrar armazenamento de dados e lógica aritmética dentro de um *chip* de silício com poucos milímetros quadrados. A idéia de incorporar um circuito integrado dentro de um cartão de identificação foi anunciada e patenteada pelos inventores alemães Jürgen Dethloff e Helmut Grötrupp em 1968. Seguiu-se uma aplicação similar pelo japonês Kunitaka Arimura em 1970. Entretanto, o primeiro progresso real veio com o anúncio da patente do cartão inteligente de Rolando Moreno na França em 1974. (RANKL; EFFING, 2000).

Nos anos 60, ocorreu o inicio do processo de utilização dos cartões inteligentes devido ao avanço da utilização de padrões de criptografia (DES, 3DES e RSA) e a expansão geral do processamento eletrônico de dados. Modernos recursos de

hardware e *software* permitiram a implementação de algoritmos matemáticos complexos que elevaram os padrões de segurança a níveis sem paralelo até então.

A partir deste avanço, estes padrões criptográficos se popularizaram e se diferenciaram da antiga criptografia. O padrão anterior de criptografia era uma ciência reservada aos círculos militares e ao serviço secreto americano. (SCHEINER, 1996).

Com a liberação dos novos recursos de criptografia, o cartão inteligente microprocessado acabou se tornando o meio ideal encontrado para garantir alto grau de segurança a diversas aplicações, pois é baseado em uma criptografia acessível a todos, uma vez que ele pode armazenar códigos secretos em segurança e pode executar algoritmos criptográficos. Além destes pontos, os cartões inteligentes são tão pequenos e fáceis de usar que eles se tornaram parte de nosso dia a dia. (RANKL; EFFING, 2000).

Sua principal característica é a incorporação de um circuito integrado no cartão, também chamado de *chip.* Este circuito integrado pode possuir funcionalidades para transmissão, armazenamento e processamento de dados, dependendo do tipo de circuito integrado que está implantado no cartão. (RANKL; EFFING, 2000).

2.2.2 Resumo Tecnológico

Os cartões inteligentes podem ser separados em várias categorias, dependendo da sua funcionalidade. Podendo iniciar em um simples cartão de memória até um cartão complexo, incluindo um microprocessador, áreas de armazenamento e processador criptográfico. (WALDER, 1997).

As características fundamentais e funções dos cartões inteligentes são normatizadas pelo Padrão ISO 7816, que divide estes cartões em duas famílias: os Cartões de Memória e os Cartões Microprocessados.

Os cartões inteligentes também podem ser classificados de acordo com o tipo

de chip e o tipo de transferência de dados, conforme mostra o gráfico abaixo: (CARDLOGIX, 2003).

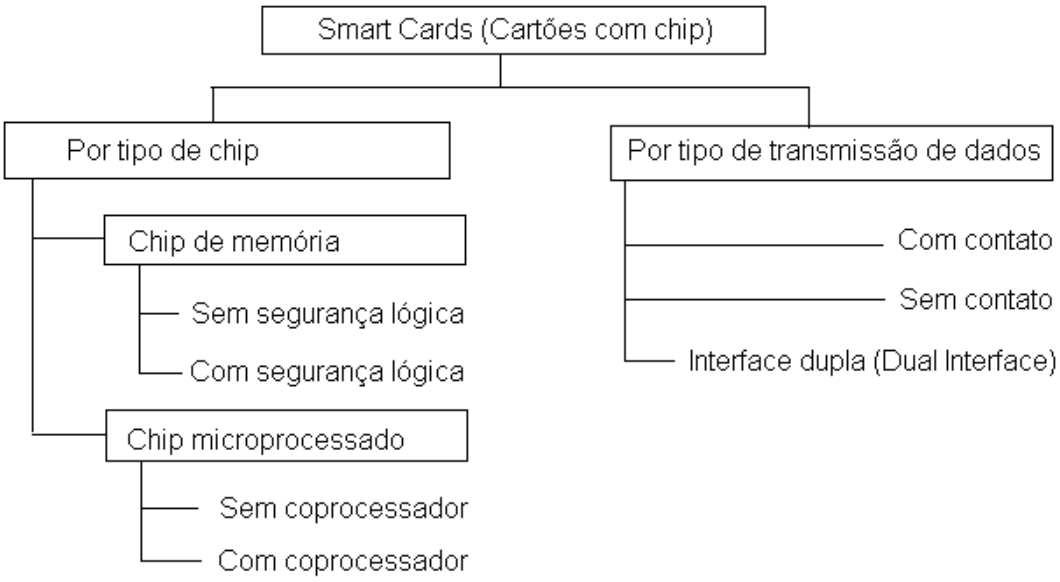


Figura 3: Estrutura da família de cartões inteligentes
Fonte: (RANKL; EFFING, 2000).

2.2.2.1 Cartões de Memória

O cartão de memória possui a arquitetura apresentada na figura abaixo.

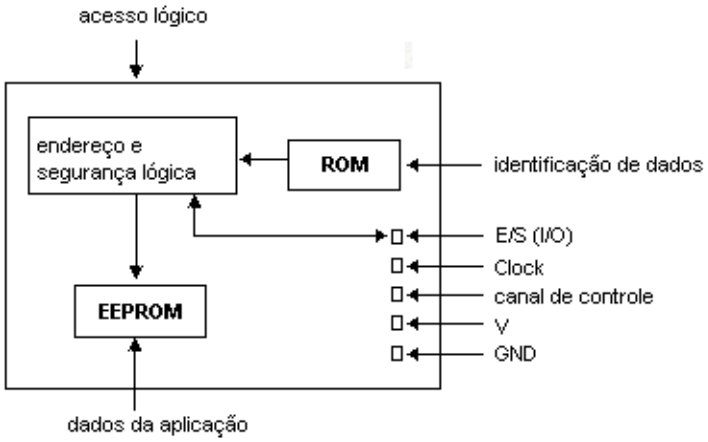


Figura 4: Arquitetura típica de um cartão memória com segurança lógica
Fonte: (RANKL; EFFING, 2000).

Os dados requeridos por uma determinada aplicação, onde os cartões inteligentes serão utilizados, são armazenados em uma memória EEPROM. O acesso à esta memória é controlado pela segurança lógica, que neste caso consiste somente na proteção contra escrita e apagamento de dados da memória. Os dados são transmitidos para o cartão através da porta de Entrada / Saída (Input/Output).

O Padrão ISO 7816 parte 3 define a utilização do protocolo de transmissão especial síncrono. (RANKL; EFFING, 2000).

2.2.2.2 Cartões Microprocessados

O cartão microprocessado possui um elemento principal que é o processador. Este processador possui 4 blocos de funções adicionais: (RANKL; EFFING, 2000).

- Mask-ROM (Mask-Read Only Memory): contém o sistema operacional do processador. O conteúdo da ROM é carregado durante o processo produtivo do cartão e não pode ser alterado durante o tempo de vida do *chip* implantado no cartão (processador);
- EEPROM (Electrical Erasable Programmable Read-Only Memory): é a memória não volátil do processador e podem conter dados e códigos de programas que são escritos e lidos com o controle do sistema operacional;
- RAM (Randon Access Memory): é a memória de trabalho do processador. Esta área é volátil e todos os dados são perdidos quando o processador não está sob uma carga elétrica;
- Porta de Input/Output (Entrada / Saída): é uma interface que realiza a transferência dos dados bit a bit. Em sua grande maioria, esta transmissão é realizada de forma serial, ou seja, em uma cadeia de bits em série.

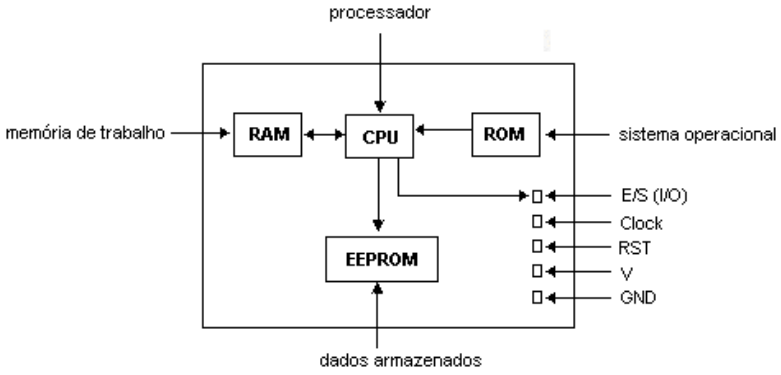


Figura 5: Arquitetura típica de um cartão microprocessado
Fonte: (RANKL; EFFING, 2000).

2.2.3 Padrões e Especificações dos cartões inteligentes

Durante os últimos 15 anos, um grande número de padrões e especificações tem sido definido, e cada vez mais aplicações sido desenvolvidas e fabricadas por diferentes fabricantes, porém sempre obedecendo a uma ou mais normas entre as que se seguem:

Padrão ISO 7816

O Padrão ISO 7816 “Cartões de identificação – Cartões de circuito integrado com contatos”, publicado pela *International Organization for Standardization* (ISO), é o padrão mais importante no que se refere as características dos cartões com *chip* (ISO 7816, 1998).

Este padrão cobre diversos aspectos de um cartão inteligente:

- Parte 1 (1998) – Características físicas;
- Parte 2 (1996) – Dimensões e localizações dos contatos;
- Parte 3 (1997) – Protocolos de transmissão e sinais eletrônicos;
- Parte 4 (1995) – Comandos entre indústrias para troca de informações;
- Parte 5 (1994) – Identificadores de aplicações;
- Parte 6 (1997) – Elementos de dados;
- Parte 7 (1997) – Comandos interindustriais para SCQL (Structured Card Query Language);
- Parte 8 (1998) – Comandos relativos a segurança interindustriais;

- Parte 9 (1998) – Comandos avançados interindustriais;
- Parte 10 (1998) – Sinais eletrônicos de solicitação e resposta para cartões síncronos;
- Parte 11 (1998) – Estrutura de cartões e funções avançadas para uso de multi-aplicações.

2.2.4 Formatos

Pequenos cartões com dimensões típicas de 85.6 mm por 54 mm têm sido usados há muito tempo. Quase todos os cartões inteligentes são produzidos neste formato, o formato mais conhecido. Ele é designado de ID-1 (Figura 7), e o seu tamanho é especificado pela norma ISO 7810. (ISO 7810, 1995).

Cabe observar que "ID", cujo significado é cartão de identificação, criado em 1985, nada tem a ver com os cartões inteligentes que conhecemos hoje em dia.

A norma ISO 7810 somente descreve o padrão ID-1 como sendo cartões de plástico com alto-relevo que trazem uma tarja magnética e que são utilizados para identificação pessoal. Sendo que na época da concretização desta norma, um *chip* incorporado ao cartão não havia sido considerado. Somente vários anos mais tarde, padrões adicionais definiram a presença de um *chip* e sua posição no cartão. (RANKL; EFFING, 2000).

De acordo com a norma ISO 7816-1, o cartão plástico deve possuir as seguintes dimensões:

- Retângulo externo: Comprimento 85.72 mm (= 3.375")
  Altura 54.03 mm (= 2.127")
- Retângulo interno: Comprimento 85.46 mm (= 3.365")
  Altura 53.92 mm (= 2.123")

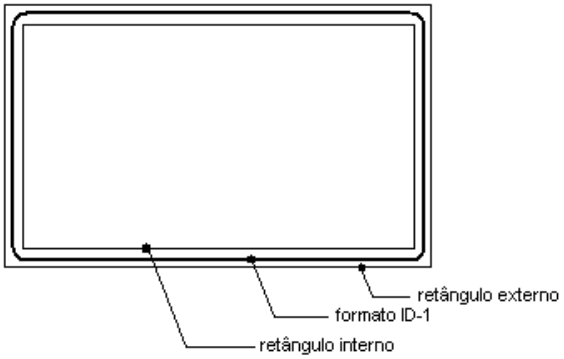


Figura 6 – Definição de dimensões do formato ID-1.
Fonte: (RANKL; EFFING, 2000).

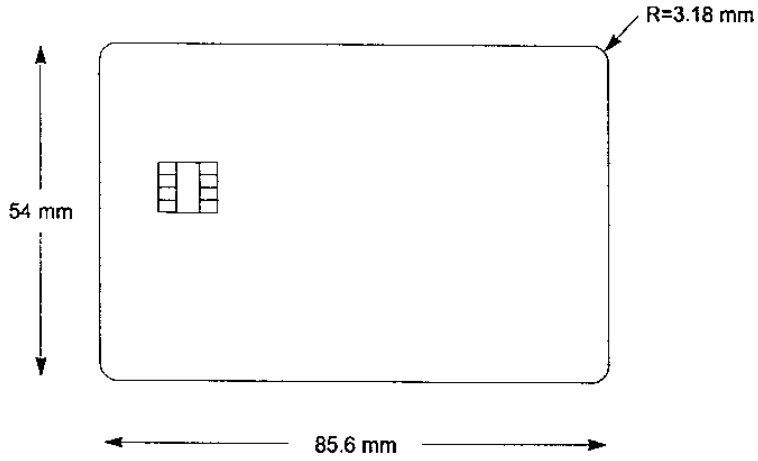


figura 7 – O formato ID-1. Espessura: 0,76 mm ±0.08 mm; raio do canto: 3.18 mm ±0.30 mm (as medidas individuais representam as dimensões sem tolerâncias).
Fonte: (RANKL; EFFING, 2000).

2.2.5 Cartões inteligentes com contato

A principal diferença entre um cartão inteligente e todos os outros tipos de cartão é o *chip* (microprocessador) que está implantado no plástico. Se o fornecimento de potência e a transferência de dados requerem um contato físico, isto é feito via um terminal elétrico que consiste de seis ou oito contatos banhados a ouro, presentes em todos cartões convencionais.

A posição desses contatos no cartão e suas dimensões são especificadas pela norma ISO 7816-2 datada de 1988. (ISO 7816, 1998).

O campo de contato é localizado no canto superior esquerdo do cartão como

mostra a figura 8.

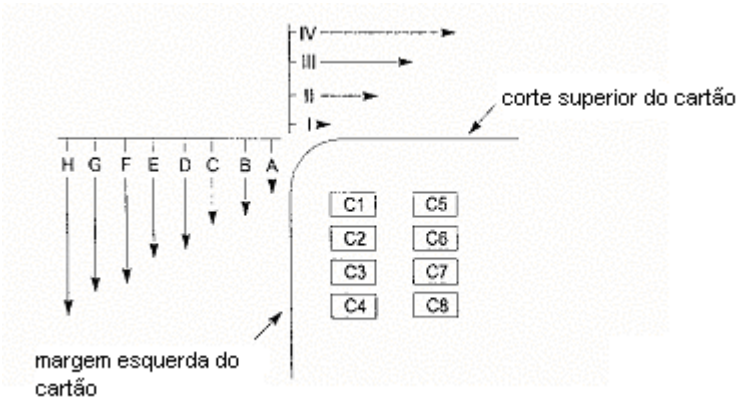


Figura 8 – Localização dos contatos em relação ao corpo do cartão (as localizações não estão em escala).
Fonte: (RANKL; EFFING, 2000).

Cada contato não deve ser menor que 1.7 mm de altura por 2mm de largura. O tamanho máximo não é especificado. Entretanto, ele é limitado pela necessidade de isolamento elétrico entre os contatos. (ISO 7816,1998).

A localização do *chip* no cartão é especificada pelos padrões da norma ISO 7816-2, conforme figura 9. Da mesma forma, a tarja magnética e o campo de alto-relevo são especificados precisamente pela norma ISO 7811. (ISO 7811, 1996).

Todos os três elementos (tarja magnética, *chip* e campo de alto-relevo) podem coexistir num único cartão. Entretanto, as seguintes regras devem ser observadas: se um cartão possuir somente um *chip* e um campo de alto-relevo, eles poderão estar localizados numa única face ou em faces opostas. (ISO 7816,1998).

Porém, se o cartão possuir uma tarja magnética, ela deve estar obrigatoriamente localizada na face oposta ao campo de alto-relevo.

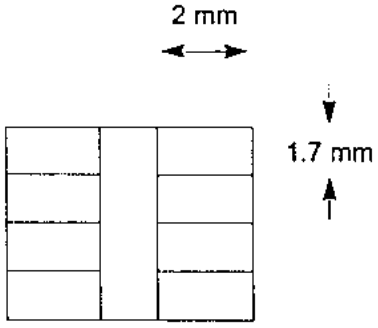


Figura 9 – Tamanho mínimo dos contatos de acordo com ISO 7816-2.
Fonte: (RANKL; EFFING, 2000).

2.2.6 O corpo de um cartão

Os materiais, o tipo de construção e de produção do corpo de um cartão é efetivamente determinado pelos elementos funcionais do cartão, bem como pelo *stress* que eles são submetidos durante o seu uso. Os elementos típicos incluem:

- Trilha magnética;
- Faixa de assinatura;
- *Embossing* (impressão de dados variáveis em alto relevo ou em termo-impressão);
- Impressão dos dados pessoais através de impressão laser;
- Holograma;
- Impressão de segurança;
- Características de autenticação invisíveis;
- *Chip* com contato ou outro elemento de união.

Os requisitos mínimos para garantir a robustez de um cartão estão descritos no padrão ISO 7810, 7813 e 7816 parte 1, e estão relacionados com os seguintes aspectos:

- Radiação Ultra Violeta
- Radiação X-ray
- Contorno da superfície do cartão
- Robustez mecânica do cartão e dos contatos

- Suscetibilidade eletromagnética
- Descarga eletrostática
- Resistência a temperaturas

2.2.7 Métodos de Produção

A produção de cartões inteligentes está no topo da tecnologia de cartões. Os fabricantes estão constantemente buscando produzir cartões mais baratos e confiáveis usando tecnologias mais rápidas.

Existem quatro estágios principais no processo de produção e inicialização: (RANKL; EFFING, 2000).

2.2.7.1. Manufatura do Corpo do Cartão

Existem dois métodos de produção de cartões plásticos: **laminação** e **injeção**.

Cartões laminados são de alta qualidade e possuem uma camada plástica transparente para proteger a arte gráfica e a superfície de impressão. Calor e pressão são usados para "colar" diversas camadas de plástico em folhas. Cartões individuais são cortados destas folhas plásticas e uma cavidade para o módulo será feita no cartão. O material mais comum utilizado nestes cartões é o PVC (*PolyVinyl Chloride)*.

Injeção envolve aquecer ABS (*Acrylonitrile-butadiene-styrol***)** a aproximadamente 250^{o} C produzindo plástico líquido. Este plástico é injetado a alta pressão em um molde, que possui cavidades com o formato do cartão. A forma é resfriada e o corpo plástico sólido do cartão é ejetado, o excesso de plástico é cortado e removido.

Após o término do processo de fabricação do cartão plástico, certa porcentagem dos cartões é escolhida para que se realizem testes de qualidade conforme indicado na norma ISO 7816. (ISO 7816, 1998).

2.2.7.2. Manufatura dos Módulos

O processo de fabricação do módulo consiste na junção do chip com a placa de ouro, que será o contato externo entre o chip e o equipamento que realizará a leitura ou gravação dos dados armazenados no cartão.

O módulo é encapsulado com resina para proteção, sendo que este processo é extremamente sensível a contaminação (figura 10). Devido a isto, várias medidas preventivas como pressão positiva de ar, antiestática e outras são utilizadas pelas empresas fabricantes dos módulos.

Depois que o módulo é montado (figura 11), ele é colado dentro da cavidade do cartão pré-impresso, através de um processo chamado *embedding* ou implantação do módulo. Todo o processo pode ser verificado na figura 12.

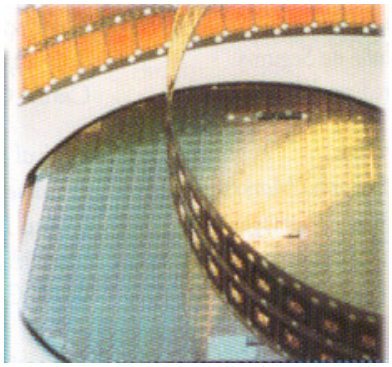


Figura 10: Placa de silício (Wafer) e rolo de chip
Fonte: (RANKL; EFFING, 2000).

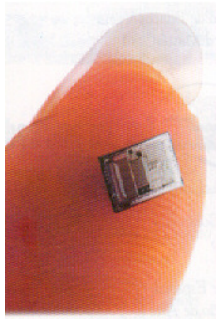


Figura 11: Microchip pronto
Fonte: (RANKL; EFFING, 2000).

Processo de Manufatura do Módulo – do Wafer ao Chip

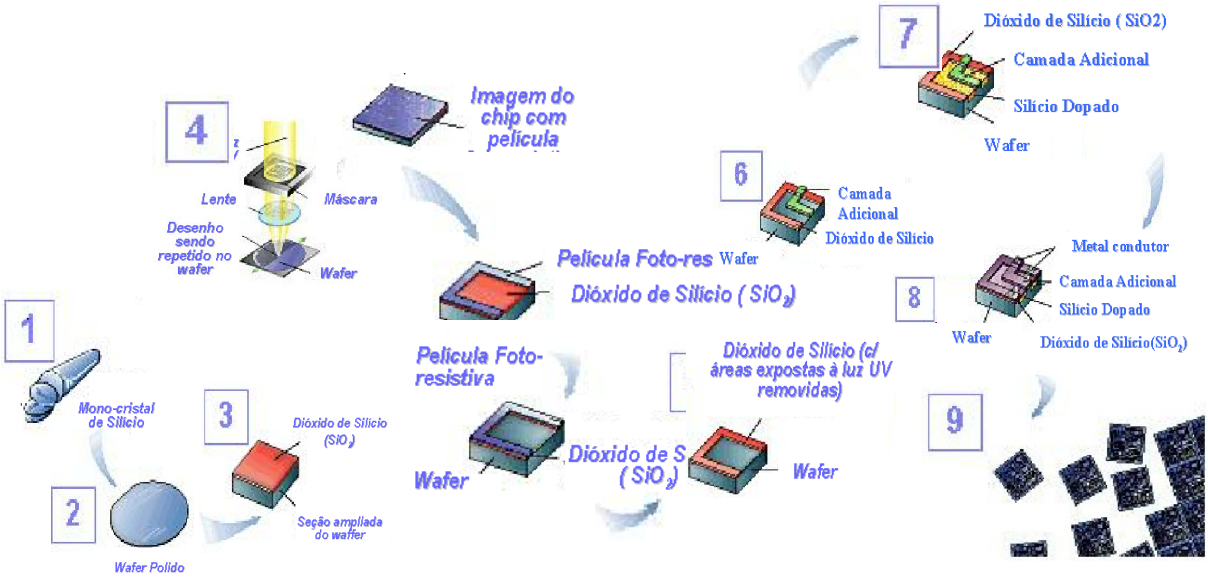


Figura 12: Processo de fabricação dos módulos

Fonte: (Infineon; 2002)

Passos:

1 – Corte do lingote de silício em lâminas;

2 – Desgaste e polimento das lâminas;

3 – Oxidação do silício;

4 – Transferência da máscara;

- 4.1 – Deposição da película fotoresistiva;
- 4.2 – Aplicação da luz UV, peça a peça;

5 – Retirada dos materiais;

- 5.1 – Película fotoresistiva
- 5.2 – Dióxido de silício da área exposta à luz UV
- 5.3 – Formato de parte do circuito do chip

6 – Processo repetitivo;

- 6.1 – Novas camadas – até 16 camadas;

7 – Implantação iônica;

- 7.1 – Mudança nas características de condutividade do silício;

8 – Deposição de camada de metal (liga alumínio) – 5/6 camadas;

- 8.1 – União entre as diversas camadas / elementos;

9 – Individualização (Back end).

Este processo demora de 8 a 17 semanas para a finalização total. (INFINEON, 2002).

2.2.7.3. Implantação do Módulo (*Embedding*)

O processo de inserção de módulos dentro das cavidades dos cartões é chamado de *Embedding* (figura 13).

Os métodos utilizados durante a manufatura do módulo e implantação têm um importante papel na confiabilidade dos cartões de circuito integrado, pois se um módulo não estiver bem conectado ao plástico, o mesmo pode se soltar e parar de funcionar.

Existem duas técnicas de implantação do módulo no cartão plástico. A primeira técnica é a mais antiga e utiliza cola líquida. A segunda técnica é mais recente e utiliza uma fita seca similar à fita adesiva de dupla face.

A cola líquida não é muito forte, especialmente quando utilizada para unir dois tipos de materiais diferentes (como metal e plástico) e pode provocar a quebra do módulo quando o cartão é dobrado ou entortado, pois a parte de trás do chip está rigidamente colada ao plástico.

A segunda técnica que utiliza colagem com fita seca foi projetada para acabar com as desvantagens das colas líquidas. Seu funcionamento é dado através da colagem de um lado da fita aderindo ao plástico e o outro lado aderindo ao metal. O correto posicionamento do adesivo pode ser garantido desde que aplicado em ambiente seco.

Este processo se torna mais forte do que as alternativas de cola líquida. Por este motivo, é necessário apenas ser aplicado atrás do contato, ao invés de aplicado atrás do chip. Isto resulta em uma bolsa de ar que protege o chip durante flexão do cartão, prolongando a vida do chip.

Neste processo de implantação são realizados os seguintes estágios:

1. A posição da cavidade é checada;

2. O posicionamento do módulo é controlado pelo equipamento;
3. O módulo é retirado da fita em um processo à vácuo;
4. Passa por um processo de aquecimento derretendo a cola na fita;
5. Realização de testes de condutividade elétrica;
6. Os cartões estão prontos para o processo seguinte que é o de personalização de dados.

(RANKL; EFFING, 2000).

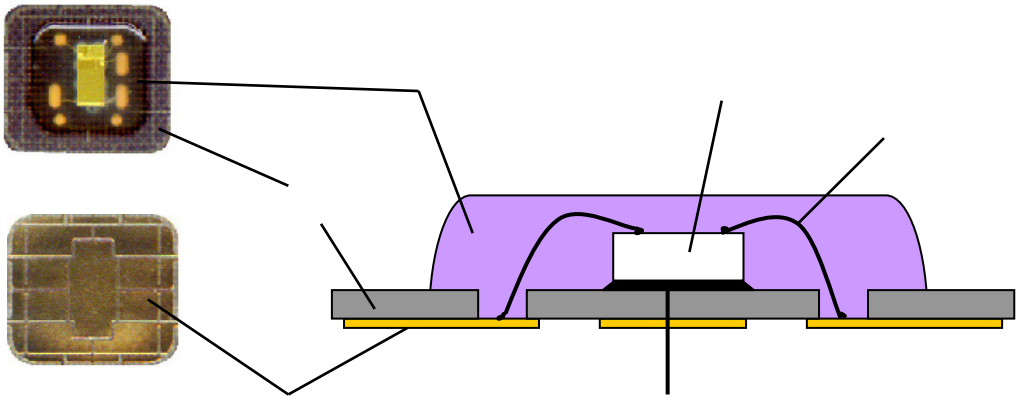


Figura 13: Instalação do módulo do chip no corpo do cartão.
Fonte: RANKL; EFFING, 2000

2.2.7.4. Estágios de Personalização

A personalização é o passo final do processo de manufatura. Este passo envolve geração, transmissão e gravação de dados, PINs (*Personal Insert Number)* e chaves de segurança criptografadas. Neste processo, geralmente é necessário que os dados estejam criptografados, pois assim, todas as informações serão tratadas com confidencialidade e confiabilidade.

Existem 3 passos de personalização:

Pré-personalização é o processo que inclui testes elétricos, criação de uma estrutura de arquivos, carregamento de dados independentes do cartão e a geração de uma chave de transporte.

Personalização é o processo que dá ao cartão uma identidade. É o único processo que envolve o cartão bem como o chip. Identificação única do cartão pode ser colocada no plástico pré-impresso por uma série de métodos: "*laser engraving*" (baixo relevo), embossamento (alto relevo), transferência termográfica e outros.

Pós-personalização é o processo realizado após o cartão ter sido entregue ao usuário final. Este processo implica em carregar novas aplicações em um cartão que já passou pelos dois processos acima e que já está sendo utilizado no dia-a-dia. Para que este processo seja realizado, o emissor do cartão necessita ter as aplicações desenvolvidas e pontos de carga onde o usuário possa levar o cartão e carregar as aplicações desejadas.

2.3 Biometria

2.3.1 Histórico

Biometria é o método de captura física de determinadas características físicas ou comportamentais do indivíduo e que podem ser, conseqüentemente, comparados com dados armazenados em um determinado local. Segundo Pódio, a definição de Biometria é "*O uso automático de características físicas ou comportamentais para determinar ou verificar a identidade de um indivíduo*". (PODIO, 2003).

A biometria, segundo Ashbourn (ASHBOURN, 2002) , existe desde os remotos tempos do Egito. De acordo com o autor, Khasekem foi o primeiro registro de utilização de métodos de identificação de indivíduos. O mesmo Khasekem utilizava a identificação de nome, idade, lugar de nascimento e ocupação, além de algumas características físicas e de comportamento dos trabalhadores que faziam parte das construções das pirâmides. Assim, ele conseguia controlar qual trabalhador fazia determinado serviço e onde ele estava.

No século XIX, vários estudiosos da época, tais como o alemão Franz Joseph Gall, o italiano Cesare Lombroso e o belga Adolphe Quetelet começaram a verificar que existiam diferenças entre as mãos e os dedos dos indivíduos, e que poderiam utilizar estas diferenças para identificar e individualizar cada um deles. A partir do estudo destas diferenças iniciaram-se as pesquisas do processo de identificação de impressões digitais.

Somente na década de 60 (1960), o processo industrial conseguiu dar sua contribuição ao processo, fabricando o primeiro leitor de mão. Este leitor foi fabricado pelos irmãos Miller, Nova Jersey / USA.

Em 1990 ocorreu o início do crescimento do mercado biométrico com a criação de grandes empresas e a criação dos padrões a serem utilizados. Isto ocasionou novos investimentos na indústria biométrica e o surgimento de novas

tecnologias. (WOODWARD; ORLANS; HIGGINS, 2003).

Atualmente a biometria está sendo utilizada em diversos setores, desde reconhecimento de indivíduos na área de segurança até transações financeiras em grandes corporações bancárias.

A grande finalidade atual da biometria é garantir a autenticidade do indivíduo, sendo que todos os sistemas de biometria utilizam três tipos básicos de autenticação: (LIU; SILVERMAN, 2003).

1. Algo que você conhece:
    - Uma senha;
    - Um identificador;
    - Uma informação pessoal.

2. Algo que você tem:
    - Um cartão chave;
    - Um cartão inteligente;
    - Um token;

3. Algo que você é:
    - A Biometria.

Destes três tipos básicos, a biometria é a ferramenta mais segura e conveniente de autenticação, pois não se pode perder ou esquecer. (LIU; SILVERMAN, 2003).

2.3.2 Métodos biométricos

Existem vários métodos biométricos atualmente em discussão. Sendo que os mesmos podem ser classificados em métodos primários, ou seja, os métodos que são mais utilizados. Ou os métodos secundários, que são aqueles que possuem

uma menor viabilidade comercial ou que ainda estão em estágios de desenvolvimento. (BIODIGEST, 2003).

Entre estes métodos, podemos listar os seguintes:

Métodos primários:

- Escaneamento digital;
- Reconhecimento facial;
- Reconhecimento de voz;
- Reconhecimento da Íris;
- Escaneamento da retina;
- Escaneamento da mão;
- Reconhecimento de assinatura;
- Reconhecimento da velocidade de digitação no teclado;
- Geometria do dedo (Verificação através da estrutura de um ou mais dedos).

Métodos secundários:

- DNA;
- Reconhecimento da orelha;
- Escaneamento das veias da mão;
- “Gait recognition” (Maneira de caminhar).

Todos estes métodos biométricos utilizam um mesmo processo padrão para a captura, armazenamento e comparação dos dados. A figura 14 mostra este processo e as etapas a serem seguidas.

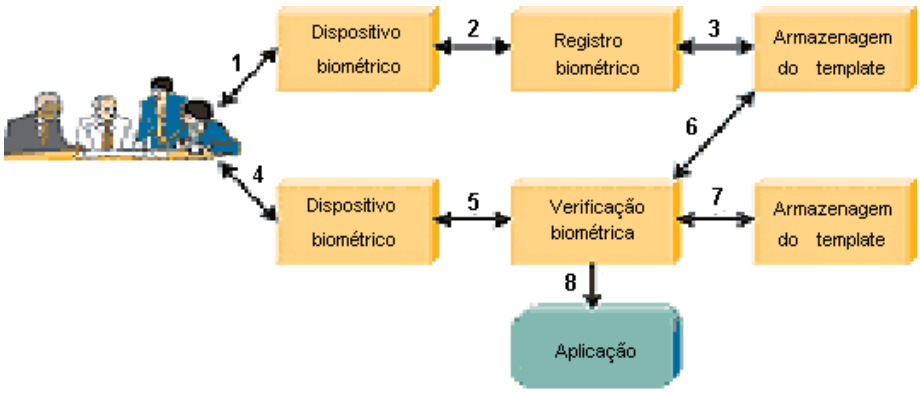


Figura 14: Processo do uso de um sistema biométrico
Fonte: (LIU; SILVERMAN, 2003).

(1) Captura a biometria escolhida;
(2) Processa a biometria, extrai e registra o modelo biométrico;
(3) Armazena o modelo em um repositório local, um repositório central ou um depositório portátil, tal como um cartão inteligente, por exemplo;
(4) Realiza a leitura (scanner) do método biométrico escolhido;
(5) Processa a biometria e extrai o modelo biométrico;
(6) Compara a biometria lida (scanner) contra a biometria armazenada;
(7) Grava um registro de auditoria com o respectivo usuário do sistema;
(8) Fornece um resultado da comparação para a aplicação que está preparada para receber a informação. (LIU; SILVERMAN, 2003).

Vale ressaltar que alguns métodos biométricos podem não ser aplicáveis para alguns usuários em determinados casos. De acordo com Struif & Scheuermann alguns casos não podem ser enquadrados no processo normal da biometria. (STRUIF, B.; SCHEUERMANN, D.; 2002),

São eles:

- Incompatibilidade cultural;
- Ausência de características biométricas;
- Características biométricas insuficientes;
- Características biométricas anormais.

Porém, ainda não existem números que nos mostre qual é o percentual de

usuários que se encaixam nestes casos, apesar de que, acredita-se que o número seja extremamente baixo e desta maneira, devem ser tratados como exceção ao processo.

2.3.3 Padrões biométricos

Para que os métodos biométricos possam ser estudados, desenvolvidos e implantados de uma forma padrão, as instituições internacionais desenvolveram um processo de padronização que resultou nas atuais normas utilizadas pela indústria, desenvolvedores de sistemas e todos os segmentos que utilizam esta tecnologia.

Estes padrões definem, principalmente, os métodos de troca de dados entre os dispositivos e a interoperabilidade da tecnologia. (PODIO, 2003).

Segue um sumário destes padrões:

Common Biometric Exchange File Format (CBEFF)

CBEFF descreve um conjunto de elementos de dados necessários para suportar tecnologias em diferentes ambientes, tais como, dispositivos móveis, cartões inteligentes, armazenamento de dados biométricos e proteção dos dados digitais. Além de facilitar o intercambio entre diferentes componentes e entre sistemas.

O *International Biometric Industry Association (IBIA)* é a autoridade registradora para este formato e todos os detalhes da CBEEF estão descritos no documento *NISTIR 6529* do *National Institute of Standards and Technology (NIST)*.

BioAPI Specification – BioAPI V1.1

A especificação *Biometric Application Programming Interface (API)* foi desenvolvida pelo *BioAPI Consortium* e é a interface entre os módulos de tecnologia biométrica e as aplicações que os utiliza.

Human Recognition Services (HRS) Module of he Open Group's Common Data Security Architecture (CDSA)

HRS é uma extensão do CDSA. Este último é um conjunto de regras de segurança e recursos de criptografia que prove a infra-estrutura para criar plataformas com interoperabilidade e segurança para ambiente cliente-servidor. O componente biométrico do CDSA HRS é usado em conjunto com outros módulos de segurança, tais como, criptografia, certificado digital e bibliotecas de dados.

X9.84-2000, Biometrics Management and Security For The Financial Services Industry

Este padrão foi desenvolvido pelo *X9.F4 Working Group of X9* e segue padrões determinados pelo *American National Standards Institute (ANSI)*. O X9.84-2000 especifica requerimentos mínimos de segurança para administração efetiva dos dados biométricos. É aplicável na segurança de captura, armazenamento, distribuição e processamento dos dados biométricos.

ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information – Fingerprint Standard Revision

Esta versão é uma revisão, designação e consolidação do padrão *ANSI/NIST-CSL 1-1993* e *ANSI/NIST-ITL 1a-1997*. O padrão especifica um formato comum a ser usado para a troca de dados de impressões digitais, faciais, cicatrizes, marcas e tatuagens entre sistemas desenvolvidos por diferentes fabricantes. Este padrão é um componente-chave para a interoperabilidade no meio judicial.

Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 11: Personal verification through biometric methods

Este padrão foi desenvolvido como a parte 11 do padrão ISO/IEC 7816. O escopo é a especificação dos processos de segurança a serem utilizados para as verificações pessoais com métodos biométricos em cartões com circuito integrado, como os cartões inteligentes. Também define os elementos de dados a serem

usados como métodos biométricos.

2.3.4 Descrição dos Métodos biométricos

2.3.4.1 Escaneamento da impressão digital

Este processo é realizado através do escaneamento da ponta do dedo e análise de pontos de verificação. Existem diversas variedades de aproximação para as verificações deste método. Alguns utilizam os métodos policiais tradicionais de comparação, outros usam dispositivos de identificação e outros ainda, utilizam métodos ultra-sônicos.

Nos equipamentos que realizam este escaneamento, alguns podem detectar quando um dedo vivo está presente, porém outros não. Devido a esta dificuldade e diferença entre os equipamentos, o processo pode ter aberturas para pequenas fraudes e falhas nos sistemas de segurança que utilizam estes dispositivos com menor nível de segurança. (LIU; SILVERMAN, 2003).

Os sistemas onde este método é utilizado com mais freqüência são geralmente os sistemas de controle de acesso físico e lógico. Principalmente porque as chances de duas pessoas (mesmo gêmeos idênticos) possuírem a mesma impressão digital é probabilisticamente menor do que 1 em 1.000.000.000 (uma em um bilhão), sendo que os sistemas utilizam os pontos de verificação para esta avaliação, conforme pode ser verificado na figura 15.,

Este método biométrico é de fácil utilização, além de garantir a segurança no processo e de ter o menor custo em relação aos demais. Assim, devido a estes fatores, ele está se tornando o método mais utilizado. (ASHBOURN, 2000).

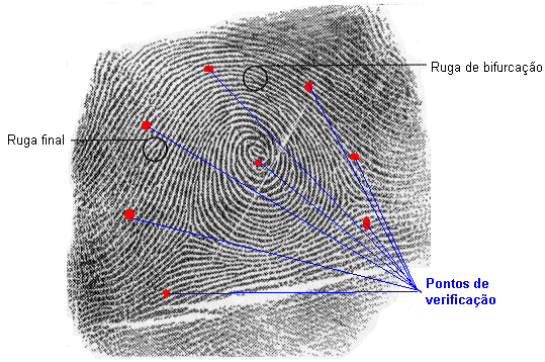


Figura 15: Impressão digital mostrando os pontos de verificação e as rugas de bifurcação e final.
Fonte: (Ashbourn, 2000).

Na digital, existem microssingularidades, chamadas *minutiae* ou *características de Galton,* determinadas essencialmente pela terminação ou pela bifurcação das linhas do cume. Os *minutiae* que combinam, constituem a base da maioria dos algoritmos para a comparação da impressão digital.

O fluxo da linha do cume pode eficazmente ser descrito por uma estrutura chamada de mapa direcional. Este mapa é caracterizado por um conjunto de matrizes ou imagens direcionais, cujos elementos denotam a orientação da tangente às linhas do cume. Analogamente, a densidade de linha do cume pode ser sintetizada usando um mapa de densidade onde se diferencia as linhas também chamadas “linha rígida” e “linha de fluxo”. (Figura 16).

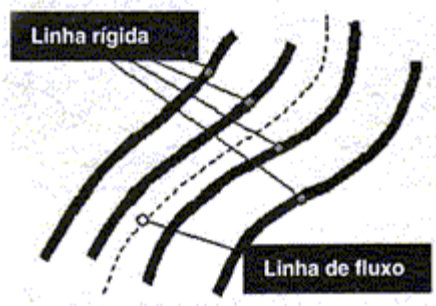


Figura 16: Diferença entre Linha rígida e linha de fluxo
Fonte: (VIGLIAZZI; 2003)

As peculiaridades da impressão digital são extraídas por um leitor de impressão e armazenadas em um banco de dados ou outro meio de armazenagem, como um cartão inteligente, permitindo, assim, uma comparação.

Em análises mais detalhadas, outras características importantes podem ser localizadas em testes de padrões de impressão digital. (Figura 17).

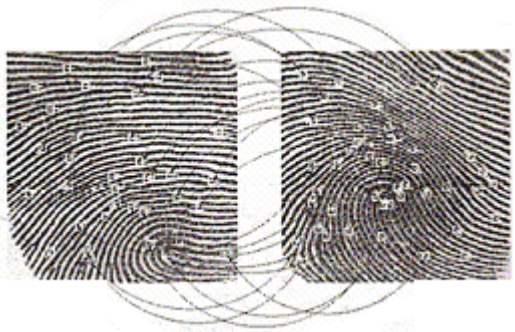


Figura 17: Comparação entre impressões digitais
Fonte: (VIGLIAZZI; 2003)

Existem, basicamente, dois métodos de leitura, o óptico e o não-óptico.

- Método Óptico: Através do método de leitura óptico, destacamos os *hologramas* e o *prisma.*

- Holograma: O dispositivo de hologramas obtém a imagem projetada refletida da impressão digital do dedo na placa lisa. Com o uso de uma placa de contato, a imagem da impressão digital é refletida na mesma, assim, através de uma projeção, o mecanismo realiza a captura da imagem.

- Prismas: O detector de prismas é um método para obter a impressão digital usando a reflexão total da luz incidindo em um conjunto de prismas. Este conjunto irá retornar ao dispositivo a imagem capturada através da reflexão da mesma contra a luz.

- Método não-óptico: É um método para obter impressão digital através da conversão da imagem em pulsos elétricos.

2.3.4.2 Reconhecimento facial

De todos os métodos biométricos, o reconhecimento facial é, sem dúvida, o mais complexo e fascinante de todos, pois consegue distinguir as diversas características faciais de diferentes indivíduos. Além de ser o mais natural, passivo e menos evasivo de todos os métodos.

As técnicas disponíveis no momento já conseguem realizar a comparação das faces independente da posição, pose, expressão, tipo de cabelo, utilização de óculos, entre outros. Isto é possível devido a utilização de diversas técnicas como visão e aprendizagem de máquina, processamento de imagens e a ciência cognitiva. (WOODWARD; ORLANS; HIGGINS, 2003).

Os sistemas de reconhecimento facial são divididos em dois grupos principais. O primeiro é o chamado “Grupo de cenário controlado” onde o objeto está posicionado em um ambiente conhecido e com uma variação mínima de cenário. O segundo é o chamado “Grupo de cenário variado” onde o objeto pode aparecer em qualquer ponto da câmera e a distâncias variadas. Em adição a estes grupos, existe ainda a funcionalidade de verificação, que pode ser uma comparação de um para um (*one-to-one match*) ou de um para muitos (*one-to-many match*).

A técnica *one-to-one* é realizada através da comparação de uma face capturada contra uma face armazenada em um banco de dados, por exemplo. A técnica *one-to-many* é realizada através da comparação de uma face capturada contra *n* faces armazenadas em um banco de dados. (ASHBOURN, 2000).

Os pontos principais de análise e comparação são os olhos, nariz, queixo, maçãs do rosto, orelhas e lábios.

O processo de identificação inicia com a captura da imagem através de uma câmera que repassa a imagem capturada para um determinado programa. Este programa fará a comparação com a foto armazenada em algum depositório de dados. A tecnologia de reconhecimento facial leva em conta as medidas do rosto que nunca se alteram, mesmo que a pessoa seja submetida a cirurgias plásticas. As

medidas básicas são: a distância entre os olhos, distância entre a boca, nariz e os olhos e a distância entre olhos, queixo, boca e linha dos cabelos.

Estas informações possibilitam identificar sósias como sendo pessoas distintas e até mesmo em casos onde a pessoa tenha modificado cor do cabelo, bigode, barba ou mesmo óculos, é possível identificar com alto grau de precisão um indivíduo.

A captura da imagem pode ser colorida ou monocromática, pois para um reconhecimento eficiente a imagem é convertida para monocromática e, logo após, todo o brilho é removido. Em seguida, é iniciado o processo de centralização dos pontos do rosto, conforme figura abaixo. (VIGLIAZZI, 2003).

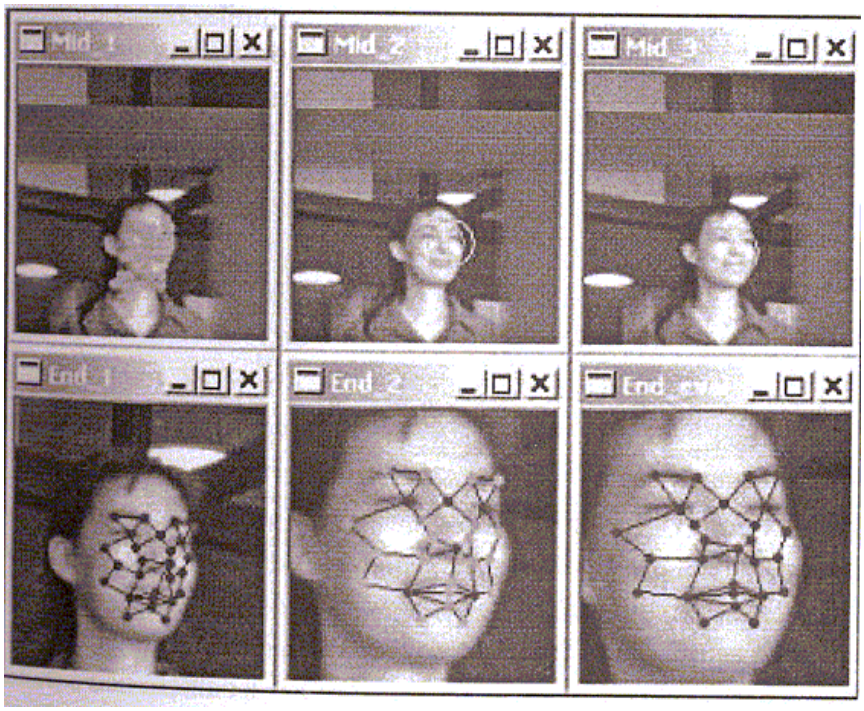


Figura 18: Etapas do reconhecimento facial
Fonte: (VIGLIAZZI; 2003)

2.3.4.3 Reconhecimento de voz

Dentre todos os métodos biométricos, este pode ser considerado o mais natural de todos, pois a voz é utilizada todos os dias, pois faz parte de nossa anatomia, e este recurso pode ser capturado pelos dispositivos e utilizado nas aplicações. (Figura 19).

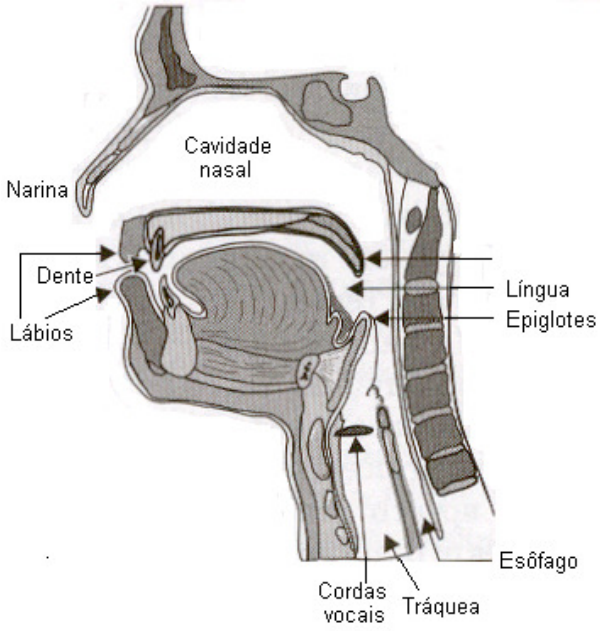


Figura 19: Anatomia da produção da fala.
Fonte: (WOODWARD; ORLANS; HIGGINS, 2003).

O aspecto principal por trás do reconhecimento de voz é a construção física das cordas vocais e os elementos adicionais de um indivíduo que afetará o dinamismo da fala. Por exemplo, se solicitarmos a dois indivíduos do mesmo sexo, estatura parecida, nascidos e criados na mesma cidade e com mesmo sotaque que falem a mesma palavra em um microfone, gravarmos e analisarmos o resultado, veremos que a análise será totalmente diferente. (ASHBOURN, 2000).

Isto ocorre, pois a autenticação da voz não está baseada no reconhecimento da voz em si, mas sim na autenticação da voz impressa, onde uma tecnologia complexa transforma voz em texto. (LIU; SILVERMAN, 2003)

Este método possui um grande potencial de crescimento, principalmente porque não exige a necessidade de equipamentos adicionais, pois a maioria dos microcomputadores atuais já possui microfones em suas configurações.

Um dos grandes problemas que afetam este método é a qualidade e o barulho do ambiente que pode afetar a verificação realizada pelo programa de comparação, pois isto pode afetar o funcionamento dos sistemas, gerando muitos erros de comparação e conseqüentemente, a não liberação dos acessos aos usuários dos sistemas.

Uma das grandes chances de utilização e melhoria para este método é a utilização do mesmo em conjunto com o escaneamento digital, pois podem substituir o uso de senhas ou cadastro de nomes, por exemplo. (LIU, 2000).

2.3.3.4 Reconhecimento da Íris

Atualmente o reconhecimento de íris está em alta, principalmente em filmes de ficção científica, como *Minority Report* e diversos outros que exploram este método para identificação do indivíduo em diversas situações.

Este método utiliza um processo de luzes infravermelhas e faz a leitura da íris do olho (Figura 20) e é desenhado para operar em um ambiente restrito e fechado. Algumas pesquisas estão sendo realizadas com câmeras especializadas que podem alcançar uma distância de 5 a 10 metros, mas estes sistemas ainda são protótipos e, portanto, não estão liberados para uso comercial.

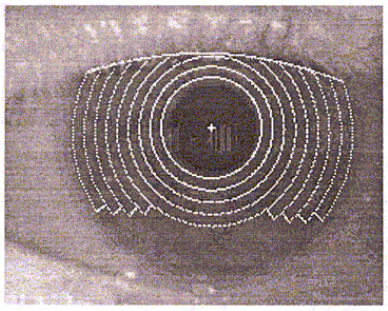


Figura 20: Processo de scaning para reconhecimento da íris
Fonte: (VIGLIAZZI; 2003)

O processo de capturar uma íris em um molde biométrico é composto de três etapas: capturar a imagem, definir a posição da íris e de otimização da imagem, e armazenar e comparar a imagem. (LIU, 2000).

- Captura da Imagem: A imagem da íris pode ser capturada usando uma câmera padrão, usando a luz visível e infravermelha, podendo ser manual ou através de procedimento automatizado.

No procedimento manual, o usuário necessita ajustar a câmera para acertar o foco na íris e necessita estar distante de seis a doze polegadas da câmera. Este processo manual é muito lento e requer o treinamento apropriado de usuário para ser bem sucedido.

O procedimento automático usa um jogo das câmeras que encontram a face e a íris automaticamente, tornando este processo de maneira muito mais amigável para o usuário.

- Posicionamento da íris e otimização da imagem: Uma vez que a câmera posicionou o olho, o sistema de reconhecimento da íris identifica a imagem que tem o melhor foco e claridade da íris. A imagem passa a ser analisada para identificar o limite exterior da íris, o limite inferior e o centro da pupila. Isto resulta na posição precisa do círculo da íris, conforme mostra a figura abaixo.

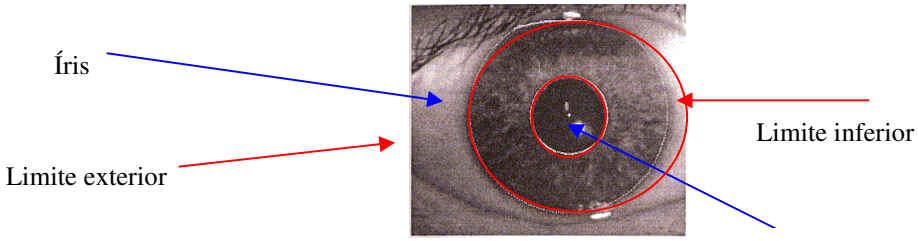


Figura 21: Posição circular da íris
Fonte: (VIGLIAZZI; 2003)

O sistema do reconhecimento da íris identifica, então, as áreas da imagem da íris que são apropriadas para a extração e a análise da informação (Figura 22). Assim, para melhorar o campo de comparação deve-se remover as áreas que são cobertas pelos cílios, sombras profundas e pelas áreas reflexivas. (WOODWARD, 2003).

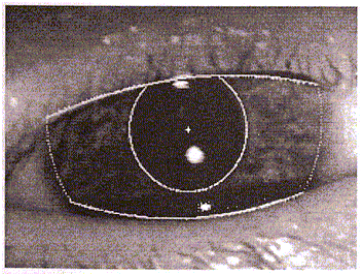


Figura 22: Otimizando a imagem
Fonte: (VIGLIAZZI; 2003)

2.3.3.5 Escaneamento da retina

O método biométrico baseado na retina envolve a análise dos vasos sanguíneos situados na parte de trás do olho. Esta tecnologia está totalmente estabilizada e sua técnica utiliza uma luz de baixa intensidade que trabalha através de uma lente ótica para escanear as características únicas da retina. (LIU, 2000).

Os dispositivos utilizados neste método já eram utilizados comercialmente antes que o reconhecimento de íris fosse realmente desenvolvido. Os grandes utilizadores desta tecnologia são as aplicações militares e as que necessitam de alto grau de segurança. Esta técnica está disponível desde o ano de 1970. (ASHBOURN, 2000).

Este método não pode ser utilizado em ambientes abertos, pois o processo requer que o usuário olhe dentro de um receptáculo binocular ou monocular e foque sua visão em um ponto central. A partir deste momento, ocorre o escaneamento das veias do fundo do olho em uma área circular de 360º, onde ocorrem 400 leituras em média para a obtenção do material (*template*) a ser armazenado. Após este processo, o *template* é reduzido a 192 pontos de referencias e armazenado em algum dispositivo para posterior comparação. (WOODWARD, 2003).

Todo este processo traz uma grande segurança ao método e garante uma identificação pessoal a prova de falhas. Esta afirmação pode ser realizada, pois, através de pesquisas, descobriu-se que a área vascular da retina é a única identificação pessoa que pode ser diferenciada, mesmo entre gêmeos idênticos. (Figuras 23 e 24).

Apesar destas afirmações, pode haver variações no processo de leitura, pois depende da saúde do usuário e de outras influencias externas. Porém, a grande vantagem deste método é que uma vez obtido um bom material armazenado para comparações não há necessidade de estar se atualizando o mesmo, como ocorre em outros métodos biométricos.

O escaneamento de retina pode ser considerado o método mais amigável para o usuário, devido a sua facilidade de uso e pela segurança do processo. Apesar de muitos usuários acharem este método danoso para a retina, isto não é válido, pois a luz emitida pelo dispositivo deve ser suficiente para penetrar no olho, iluminando a retina para que se possa ter uma imagem perfeita. Este método é indicado para aplicações que exigem um alto nível de segurança. (ASHBOURN, 2000).

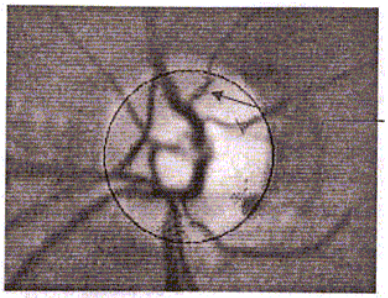


Figura 23: Identificação dos vasos sanguíneos e mapeamento completo
Fonte: (VIGLIAZZI; 2003)

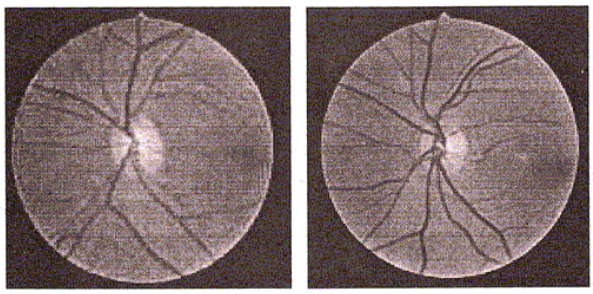


Figura 24: Retinas de irmãos gêmeos
Fonte: (VIGLIAZZI; 2003)

2.3.4 Processo de seleção de um método biométrico

Não é possível indicar qual é o melhor método biométrico, assim como não é possível afirmar que exista um método melhor do que o outro, pois para que se possa identificar qual é o melhor método biométrico, deve-se avaliar qual é a aplicação que está querendo utilizá-lo e analisar qual o método mais adequado para esta determinada aplicação.

Somente com a avaliação final da aplicação onde o método será utilizado, do

nível de segurança, das condições físicas, das características humanas, entre outros, é que se pode indicar o método mais adequado a ser utilizado.

Diferentes tecnologias podem ser apropriadas para diferentes aplicações, dependendo das necessidades dos sistemas, da base de dados, das condições ambientais, e de parâmetros específicos de cada um destes métodos.

A tabela 1 mostra uma comparação entre os métodos biométricos citados anteriormente. (LIU, SILVERMAN; 2000).

Características	**Digital**	**Facial**	**Voz**	**Íris**	**Retina**
Facilidade de uso	Alto	Médio	Alto	Médio	Alto
Incidência de erros	Umidade Sujeira Idade	Iluminação Idade Óculos Cabelo	Barulho Resfriado Tempo	Iluminação Poeira	Óculos
Precisão	Alto	Alto	Alto	Muito alto	Muito alto
Aceitação pelo usuário	Médio	Médio	Alto	Médio	Alto
Nível de segurança	Alto	Médio	Médio	Muito alto	Muito Alto
Estabilidade a longo prazo	Alto	Médio	Médio	Alto	Alto

Tabela 1: Comparação de métodos biométricos

Fonte: (LIU, SILVERMAN; 2000).

2.4 Certificação Digital

A certificação digital só foi viabilizada com a criação das estruturas de criptografia de chaves públicas. Estas estruturas foram concebidas em 1976 por W.

Diffie e M.E. Hellman e em 1977, R. Rivest, A. Shamir e L. Adleman desenvolveram o sistema de criptografia RSA (Rivest, Shamir e Adleman), considerado o primeiro sistema de chaves públicas.

Criptografia de chaves públicas pode ser um processo importante para auxiliar serviços de segurança, principalmente nos itens que incluem confidencialidade, autenticação e integridade. (HUNT, 2001)

Para definirmos o que é certificado digital, podemos utilizar a definição da CERTISIGN: “Credencial eletrônica, não palpável, gerada por uma Autoridade Certificadora que consiste em um par de senhas que permite ao titular se autenticar como autor da mensagem para o seu destinatário ou embaralhar o conteúdo de suas mensagens para que elas cheguem intactas e não lidas ao destinatário”. (CERTISIGN, 2002)

Para isto, o certificado digital possui os seguintes componentes: (HUNT, 2001); (CERTISIGN, 2002).

- Chave pública;
- Validade da chave pública;
- Autoridade Certificadora (AC);
- Número de série do certificado;
- Assinatura digital da AC;
- Política de segurança;
- Autoridade registradora (AR);
- Repositório do certificado;
- Aplicações disponíveis para a utilização dos certificados.

- Chave pública – Uma chave matemática que pode ser disponibilizada publicamente e que é usada para verificar assinaturas criadas com a chave privada correspondente. Dependendo do algoritmo, a chave pública também pode ser usada para criptografar mensagens ou arquivos que possam então ser decriptografados com a chave privada correspondente.

- Validade da chave pública – é a data limite para que a chave pública possa ser utilizada.

- Autoridade Certificadora (AC) – Empresa que emite certificados digitais obedecendo às práticas definidas na CPS (Certificate Practice Statement).

- Número de série do certificado – é o número que é liberado pela AC para cada certificado emitido.

- Assinatura digital da AC – Recurso do certificado digital que permite ao seu titular enviar mensagens eletrônicas de modo que sua identidade possa ser verificada e reconhecida pelo destinatário.

- Política de segurança – define o nível de organização e segurança da informação, bem como os processos e princípios para o uso da criptografia. Alguns sistemas de criptografia seguem as definições detalhadas por um CPS.

- Autoridade registradora (AR) – é a entidade que provê a ligação entre o usuário e a AC. É a responsável pela autenticação da identidade dos usuários e submete os certificados requeridos para a AC.

- Repositório do certificado – é o provedor do mecanismo de armazenamento das chaves e certificados.

- Aplicações disponíveis para a utilização dos certificados – são as aplicações que provêem um processo de segurança, que necessitam de confidencialidade, integridade e autenticação dos dados.

A figura 25 mostra a relação entre algumas aplicações, infra-estrutura e os padrões dos certificados digitais.

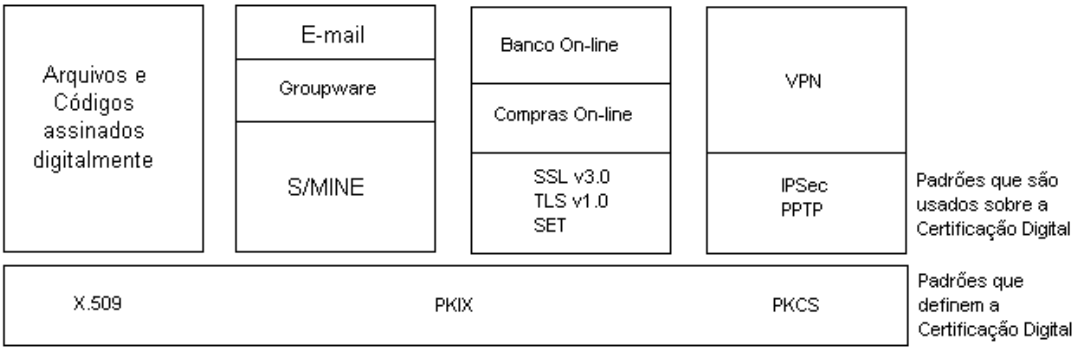


Figura 25: Funções da Infra-estrutura de Chaves Públicas para Certificação Digital
Fonte: (CERTISIGN, 2002).

A infra-estrutura de distribuição de chaves e certificados é necessária para suportar o uso destas informações em uma rede pública, como por exemplo, a Internet. A certificação digital é a combinação de diversos itens, tais como, *hardware, software*, produtos, políticas, procedimentos e padrões.
Assim, foram desenvolvidos vários padrões que devem ser seguidos como mostra a figura 25.

O padrão X.509 (Internet X.509 Public Key Infrastructure Certificate) é um dos principais padrões que gerenciam e provém o uso básico para definição dos formatos de dados e procedimentos para a distribuição de chaves públicas e certificados que são assinados digitalmente pelas Autoridades Certificadoras. (Younglove, 2001).

Este padrão não especifica um algoritmo particular de criptografia, mas o padrão em documentos anexos descreve o algoritmo RSA. O padrão X.509 é suportado por um grande número de protocolos, incluindo os protocolos padrão PKCS. (RSASecurity, 2004).

O padrão PKCS (Public-Key Cryptography Standards) define os protocolos que devem ser utilizados no processo de certificação digital. Este padrão foi desenvolvido pelos laboratórios RSA em cooperação com um consórcio informal, incluindo as empresas Apple, Microsoft, DEC, Lotus, Sun e o MIT. Os padrões publicados são os PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12 e #15. Os padrões PKCS #13 e #14 estão em desenvolvimento. (RSASecurity, 2004).

De todos os números do PKCS, o PKCS#10 é o que define o formato das mensagens e como o certificado digital pode ser utilizado em desenvolvimentos paralelos. (HUNT, 2001).

3. DESENVOLVIMENTO

Este trabalho propõe um modelo de utilização da junção dos métodos biométricos com a utilização de cartões inteligentes para a autenticação de usuários para sites de ensino à distância. Não será desenvolvido um modelo final, a proposta é mostrar o desenho de uma solução, para que se possa, posteriormente, desenvolver a aplicação final.

A sugestão para este modelo deve-se principalmente ao grande crescimento que o acesso à Internet obteve nos últimos anos e com isto, o crescimento dos problemas de segurança, que atualmente podem ir desde o roubo de senhas até a clonagem de sites.

O problema de como garantir a autenticidade do acesso do usuário de sites de ensino à distância levou a uma busca de soluções que pudessem atender as exigências do problema, pois somente a utilização de senhas para acessar os sites não garante mais a autenticidade de um usuário, pois além das falhas de segurança, como por exemplo, a descoberta da senha de um usuário, o que poderia resultar em acessos indevidos ao site, o usuário pode esquecer ou perder a senha, o que geraria grandes problemas para o mesmo.

Existem dois aspectos que levam a discussão do processo de autenticidade do usuário. O primeiro é de quando o usuário quer receber o conteúdo solicitado de maneira legítima, e para isto, todas as informações solicitadas devem ser enviadas, verificadas e retornadas de forma correta. Assim, caso exista alguma informação incorreta, o usuário nunca terá o retorno da informação solicitada e não poderá ser atendido em seu pedido.

O segundo aspecto é de quando o usuário quer fraudar o sistema. Neste caso, ele pode tentar burlar o processo de solicitação e envio de informações para que o sistema gere um erro ou que ele consiga o acesso às informações desejadas de forma ilícita, como por exemplo, a quebra de uma senha. Além destes, tem o aspecto do usuário legítimo querer fraudar o sistema repassando seus dados para

que outro usuário tenha acesso ao conteúdo do site.

Devido a isto, a proposta é a da utilização da autenticação do usuário, que consiste na verificação da identidade tanto dos usuários quanto dos processos envolvidos através dos mecanismos de métodos biométricos e de informações armazenadas em cartões inteligentes. Conforme já descrito anteriormente, os mecanismos de autenticação do usuário dividem-se em três categorias, ou seja, o que se sabe (senha), o que se tem (cartão inteligente) e o que se é (método biométrico).

Vários estudos foram realizados para verificar o processo de autenticação utilizando métodos biométricos e cartões inteligentes. Dentre estes estudos, o estudo de Hung-Min Sun (SUN, 2002), mostra a utilização do cartão inteligente para autenticar o usuário em acesso remoto que oferece várias vantagens, entre elas, a redução significativa de custos computacionais e de comunicação devido a diminuição de verificação *on-line* das informações, que estão armazenadas no cartão.

O estudo de M.S. Hwang e L.H. Li (HWANG; LI, 2000) propõe a utilização de cartões inteligentes para a autenticação remota de usuários utilizando o armazenamento da senha do usuário em *templates* criados no cartão inteligente. Estes *templates* são arquivos criados internamente no *chip* do cartão, onde podem ser armazenadas diversas informações, entre elas, a senha. Estas informações não se perdem pois estão armazenadas na área EEPROM do *chip*. Esta área é uma área de armazenamento não volátil, ou seja, não existe a possibilidade de perda de dado, a menos que isto seja definido pela aplicação que está usando os dados.

Outro estudo realizado por Raul Sanchez-Reillo (SANCHEZ-REILLO, 2001) propõe a união de cartão inteligente e métodos biométricos para garantir a autenticidade do usuário, porém, com diferentes resultados devido aos métodos utilizados (reconhecimento de voz, geometria da mão e escaneamento de íris).

Com base nestes estudos, pode-se verificar que é viável a união do cartão inteligente associado à biometria para garantir a autenticação do usuário ao site da

Internet e trazer outras vantagens, como a rapidez na autenticação e diminuição do uso da rede de comunicação. Porém, nenhum destes estudos analisou a utilização destes métodos em sites de EAD.

Além da autenticação do usuário no momento do seu acesso ao site de EAD, este modelo pode ser replicado para uso em módulos internos do sistema, ou seja, para aumentar a garantia do processo, o sistema de EAD pode usar este mesmo método para autenticar o usuário em momentos distintos dentro do sistema.

O sistema de EAD pode solicitar a autenticação do usuário antes de consultas a conteúdos específicos, durante a resposta de exercícios ou provas, acesso a informações confidenciais, autenticação temporal, ou seja, de acordo com um tempo estipulado pelo sistema, o mesmo solicita ao usuário que apresente seus dados para que os mesmos possam ser autenticados. Assim, o sistema saberá que o usuário realmente é o detentor do acesso e é ele que fisicamente presente na estação de trabalho.

Para que não haja necessidade de consultas on-line a Entidade Certificadora, no momento de verificação interna, o processo de autenticação poderá solicitar somente a identificação do usuário e realizar a verificação dos dados apresentados diretamente com os dados armazenados no cartão. Assim, toda a verificação será feita off-line, sem a necessidade de requisição de consultas à Entidade Certificadora, o que agiliza o processo de autenticação.

3.1 Modelo proposto

O modelo proposto será descrito utilizando a linguagem UML conforme descrito a FOWLER e MATOS (FOWLER, 2000) e (MATOS, 2002). Os modelos de “Diagrama de caso de uso”, “Descrição de caso de uso”, “Diagrama de classe” e “Diagrama de seqüência” encontram-se no item “Anexos” deste trabalho.

3.2 Descrição do sistema

De acordo com a estrutura definida do diagrama de seqüência, a sugestão para a apresentação da “Janela de entrada de dados” é a definida na figura abaixo.

Figura 27: Tela de entrada de usuário
Proposta de tela a ser utilizada pelo sistema em desenvolvimento.

Nesta tela, deverão ser apresentados os seguintes dados, de acordo com a seqüência de solicitação:

1. Usuário;
2. Senha;
3. Inserção do cartão na leitora de cartões;
4. Posicionamento do dedo na leitora de biometria.

Os passos de verificação deverão ser seguidos e caso ocorra algum problema

em alguma etapa, as mensagens definidas do Diagrama de Caso de Uso deverão ser mostradas ao usuário.

No processo de solicitação de dados, a requisição da senha foi proposta para que fosse seguido o processo de autenticação sugerido por (LIU, SILVERMAN, 2003), ou seja, apresentar as informações sobre “Algo que você conhece” (Senha), “Algo que você tem” (Cartão) e “Algo que você é” (Biometria).

3.2.1 Definição do template do cartão

O *template* do cartão corresponde a estrutura que os dados terão para serem armazenados no cartão.

Cada dado tem sua característica e a estrutura dos dados segue o padrão ISO 7816 – 1, que define a estrutura de *Master File* (MF), *Direct File* (DF) e *Elementary File* (EF).

Para criar a estrutura do cartão, foi utilizado o *software* STARMAG da empresa fabricante de cartões *Giesecke & Devrient GmBH* e o cartão com características biométricas STARCOS SPK 2.4 Este software possibilita a criação da estrutura de acordo com os requisitos da norma ISO 7816-1.

Os dados principais que estarão armazenados no cartão serão:

- Nome do usuário;
- Senha do usuário;
- Impressão digital;
- Certificado digital.

Estes dados estarão armazenados em arquivos distintos (EF), porém fazendo parte de um mesmo diretório (DF). Conforme pode ser verificado na figura 28, a estrutura do cartão segue uma formatação em *árvore*, iniciando no diretório principal MF (*Master File*).

Este diretório por sua vez, é subdividido em outro diretório, que possui a

denominação DF (*Directory File*). Este diretório possui uma chave de acesso para as funções de leitura e gravação. Esta chave é representada pelo arquivo ISF (*Internal Secrety File*). Somente com o conhecimento desta chave é possível fazer as operações de leitura e gravação dos dados armazenados nos arquivos abaixo deste diretório. Esta estrutura pode ser observada na figura 28.

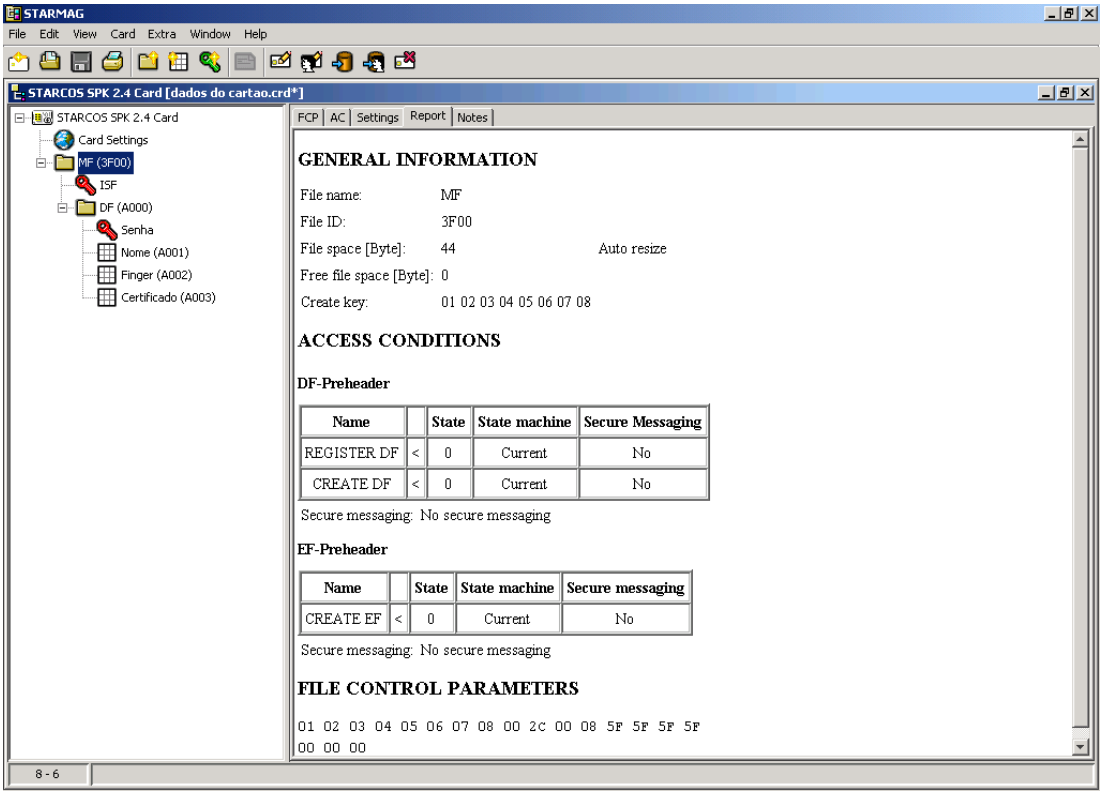


Figura 28: Estrutura completa do cartão
Estrutura desenvolvida utilizando o software STARMAG G&D

O diretório DF é subdividido pelas quatro informações que serão utilizadas pelo sistema e que devem ser gravadas no cartão. Estas informações, já descritas acima, são definidas de acordo com as regras da norma ISO e são consideradas arquivos. Cada arquivo possui sua característica, como tamanho, regra de acesso, etc.

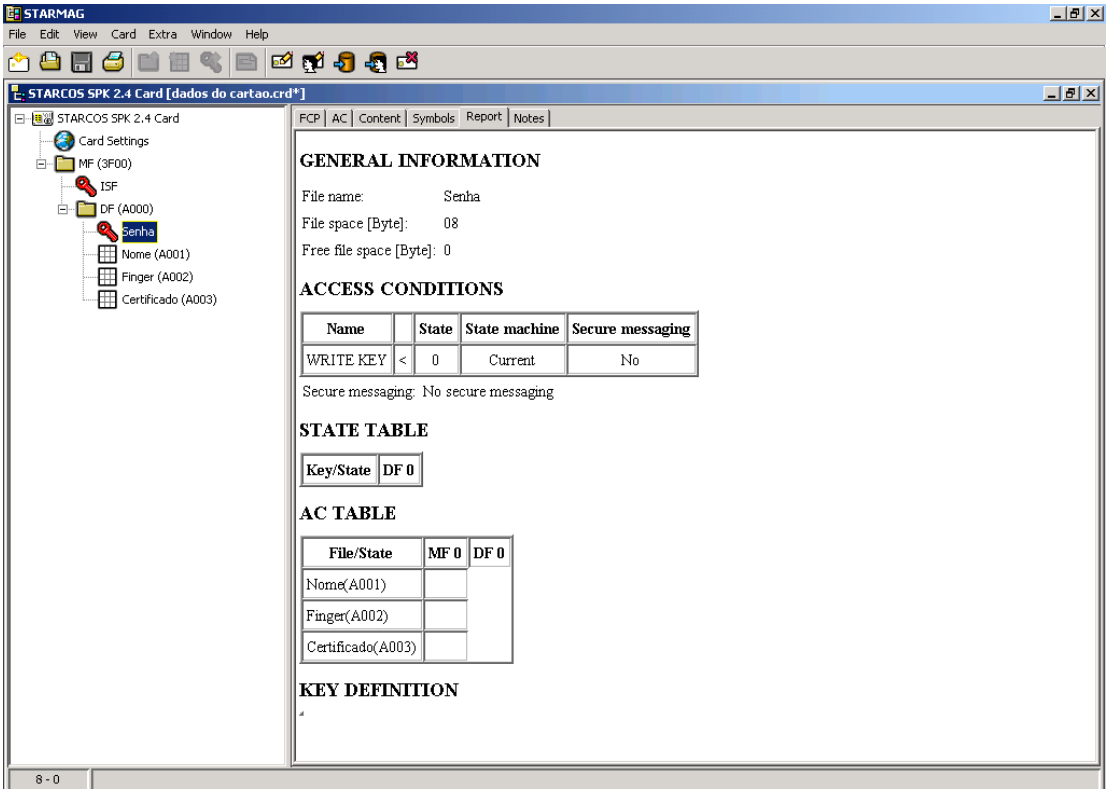


Figura 29: Estrutura do campo SENHA

Estrutura desenvolvida utilizando o software STARMAG G&D

A informação SENHA é um arquivo onde será armazenada a senha do usuário. Conforme figura 29, as características deste arquivo são:

- Tamanho do campo: 8 bytes
- Condição de acesso: Chave de gravação.

  Para esta condição de acesso só são permitidos os processos de leitura e gravação. Não é permitido apagar esta informação.

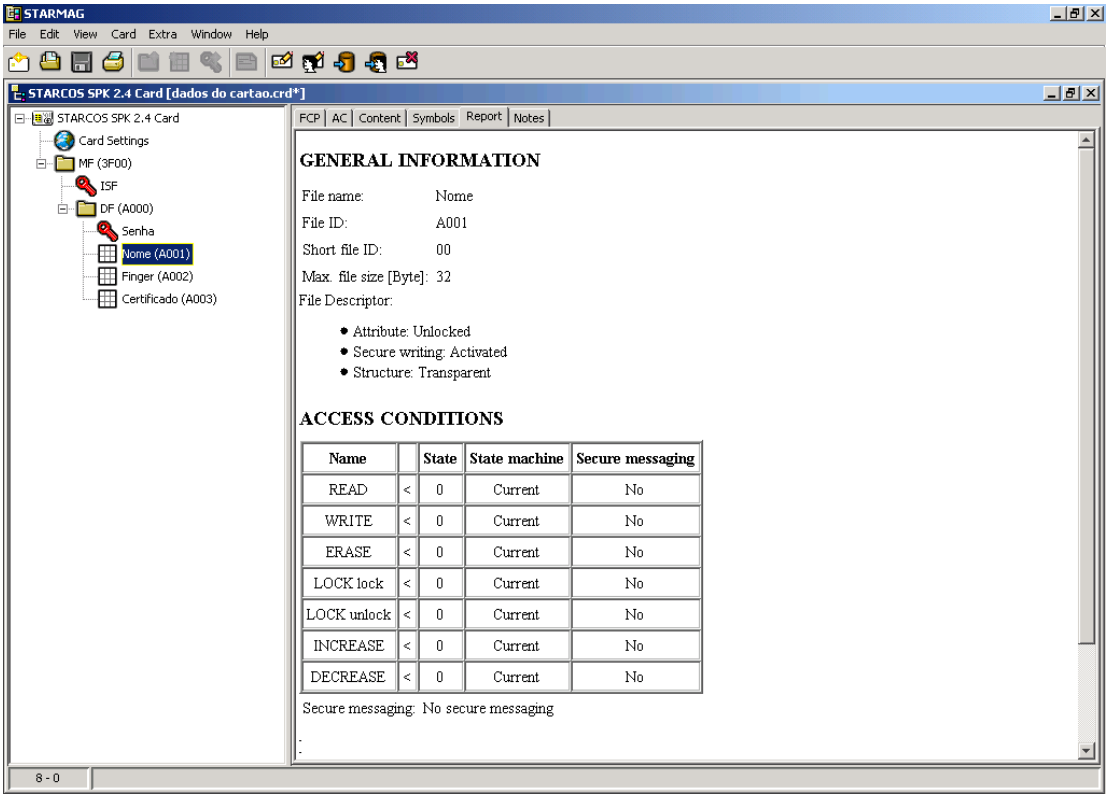


Figura 30: Estrutura do campo NOME

Estrutura desenvolvida utilizando o software STARMAG G&D

A informação NOME é um arquivo onde será armazenado 0 nome do usuário. Conforme figura 30, as características deste arquivo são:

- Tamanho do campo: 32 bytes
- Identificação do arquivo: A001
- Condição de acesso: Neste arquivo é permitida a leitura, gravação, exclusão, bloqueio dos dados, incremento e decremento de dados.

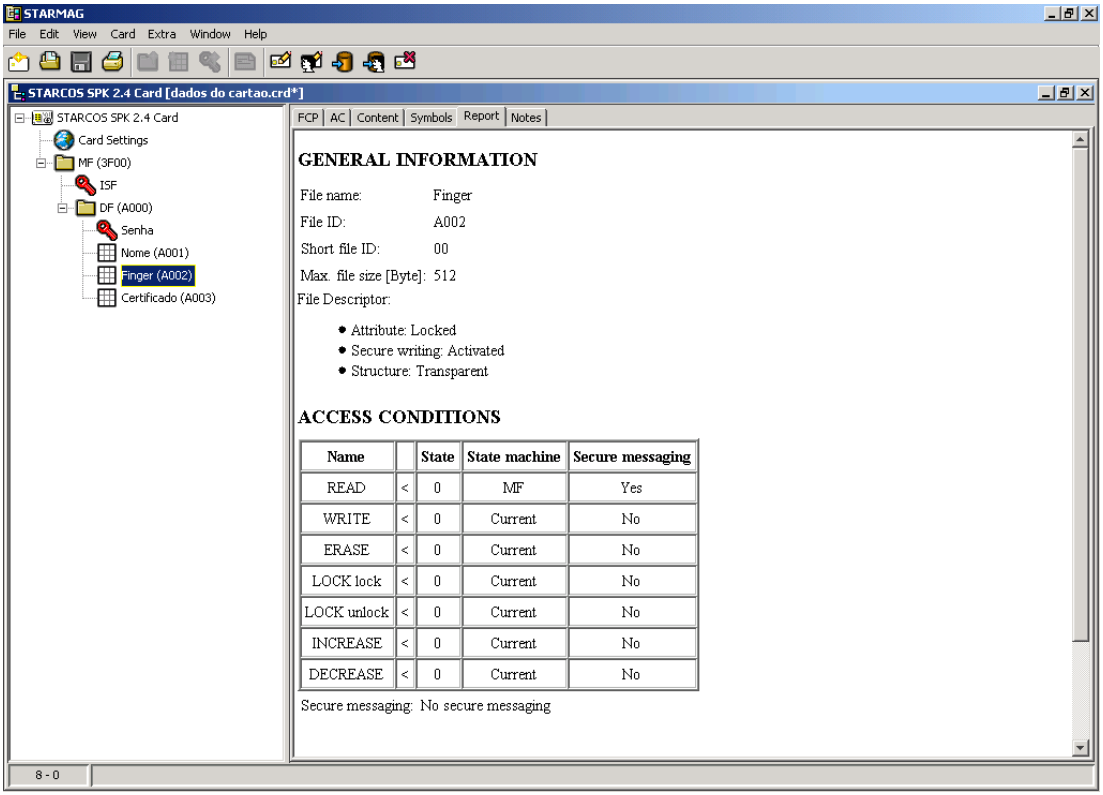


Figura 31: Estrutura do campo FINGER

Estrutura desenvolvida utilizando o software STARMAG G&D

A informação FINGER é um arquivo onde será armazenado a digital do usuário. Conforme figura 31, as características deste arquivo são:

- Tamanho do campo: 512 bytes
- Identificação do arquivo: A002
- Condição de acesso: Neste arquivo é permitida a leitura, gravação, exclusão, bloqueio dos dados, incremento e decremento de dados.

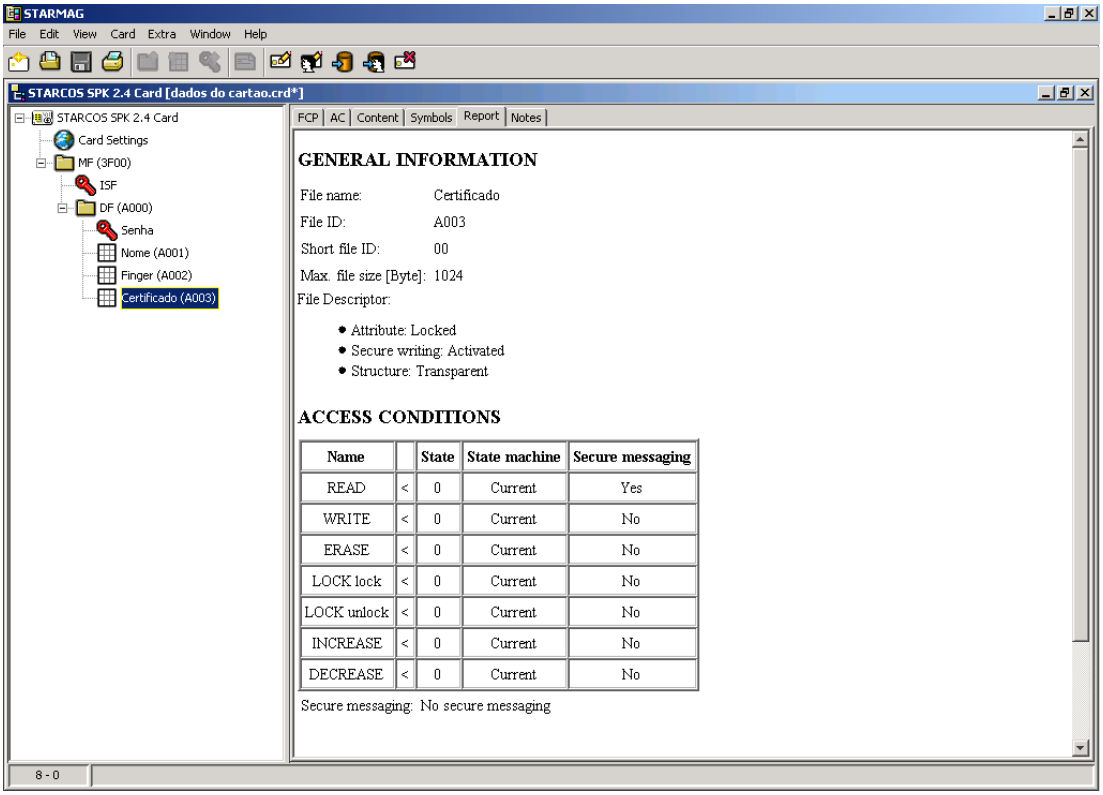


Figura 32: Estrutura do campo CERTIFICADO

Estrutura desenvolvida utilizando o software STARMAG G&D

A informação CERTIFICADO é um arquivo onde será armazenado o certificado digital do usuário. Conforme figura 32, as características deste arquivo são:

- Tamanho do campo: 1024 bytes
- Identificação do arquivo: A003
- Condição de acesso: Neste arquivo é permitida a leitura, gravação, exclusão, bloqueio dos dados, incremento e decremento de dados.

As informações do *template* do cartão serão utilizadas pelas chamadas de funções, que terão a responsabilidade de leitura e gravação dos dados no cartão.

Com todas estas informações armazenadas no cartão, ou seja, o nome do usuário, sua senha, seu certificado e sua biometria, o sistema aumentará o nível de segurança do processo, inclusive diminuindo o fluxo de informações na rede, visto que as verificações relativas aos dados do usuário serão realizadas diretamente com os dados armazenados no cartão. Assim, o sistema terá a segurança necessária para garantir que o usuário que está a frente do computador, é o usuário que

realmente deveria estar acessando o sistema.

A sugestão de utilização das três informações do usuário (nome, senha e biometria) é para aumentar o grau de segurança do sistema, pois o usuário terá que se autenticar com mais dados e quanto mais informações forem solicitadas, maior o nível de segurança que é agregado ao sistema.

A biometria é o ponto crucial deste processo de segurança, pois é ela que irá dar a confirmação final da legalidade do usuário. Caso outro usuário consiga as duas primeiras informações, ele não terá a terceira (biometria) para poder se autenticar no sistema, assim, o fraudador não poderá se passar pelo usuário legítimo.

3.2.2 Estrutura básica das chamadas de função

O processo de chamadas das funções deve possuir a seqüência descrita abaixo. Não há necessidade de se ter uma linguagem de programação específica para que se desenvolva as funções e a base do programa principal.

A função principal do sistema será responsável pelas chamadas das funções secundárias e de todo o tratamento dos valores de retorno das outras funções. Para verificar os detalhes da Função Principal, verificar a mesma no item “Anexos”.

3.2.3 Definição da função Consulta_usuário()

Esta função é responsável pela consulta dos dados cadastrados no *template* do cartão. Ela deverá retornar a Função Principal as informações sobre a consulta dos dados do usuário.

Como resultado da consulta, esta função irá retornar o valor “1” caso o nome recebido não seja igual ao nome armazenado no cartão. Caso a Senha recebida não seja igual a Senha armazenada no cartão, esta função deverá retornar o valor “2”.

Para verificar os detalhes desta, verificar a mesma no item “Anexos”.

3.2.4 Definição da função Verifica_certificado()

Esta função verifica o certificado digital armazenado no cartão contra o certificado armazenado na Certificadora (CA) responsável pela geração do certificado.

Para verificar o certificado, esta função irá recuperar o certificado público e enviará o mesmo para a Autoridade Certificadora (CA) onde receberá a informação se o certificado realmente é valido. Com base nestas informações, a função retornará à Função Principal o resultado “1” em caso de data de expiração do certificado e o valor “2” em caso de certificado inválido.

Para verificar os detalhes desta, verificar a mesma no item “Anexos”.

3.2.5 Definição da função Verifica_reg_cartão()

Esta função é responsável pela verificação do cadastro do cartão no banco de dados do sistema.

Ela realizará a leitura do número do cartão e enviará os comandos de acesso ao banco de dados e o comando de leitura da informação desejada no mesmo.

Caso o cartão não esteja cadastrado no banco de dados, a função irá retornar o valor “1” para a Função Principal.

Para verificar os detalhes desta, verificar a mesma no item “Anexos”.

3.2.6 Definição da função Compara_template()

Esta função é responsável pela captura da digital e pela comparação da mesma com a digital armazenada no template do cartão.

Caso a digital capturada não seja igual a digital armazenada no cartão, a função deverá retornar o valor “1” para a Função Principal.

Para verificar os detalhes desta, verificar a mesma no item “Anexos”.

3.3 Processo físico

O processo físico consiste na ambientação do sistema e dos dispositivos que o mesmo deverá possuir para que tenha seu funcionamento realizado de forma funcional.

Para que o ambiente seja configurado para seu total funcionamento, o mesmo deverá ter as seguintes características:

- Microcomputador com processador mínimo compatível com Pentium III, memória mínima de 128 Kbytes. Sistema operacional mínimo Windows 98;
- Leitora de cartões com capacidade de sensor biométrico e leitura de cartões inteligentes com contato atendendo a norma ISO 7816 com conexão USB ou RS-232;
- Cartão inteligente com contato com características biométricas atendendo as normas ISO 7816.

A figura 33 mostra um modelo de como deverá ser composto o ambiente. Não está no escopo deste projeto a definição do sistema de retaguarda da aplicação, nem a definição de qual produto a ser utilizado. O processo é somente ilustrativo para que possamos ter a idéia de como o sistema funcionará após o término do seu desenvolvimento.

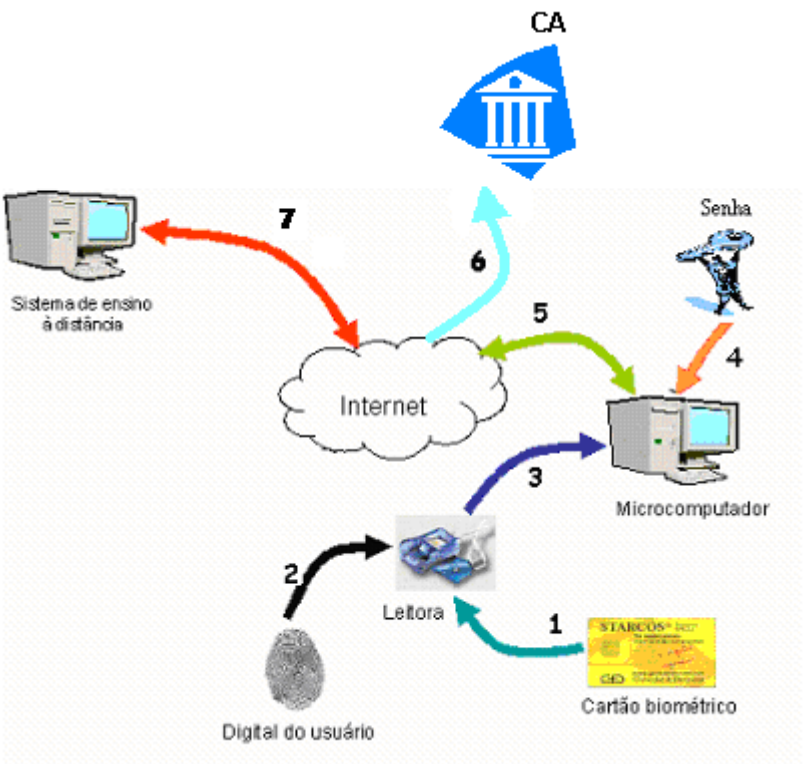


Figura 33: Estrutura do processo físico
Estrutura desenhada para o desenvolvimento desta proposta.

Neste processo, o fluxo da informação deverá seguir da seguinte maneira:

1. O Usuário insere o cartão na leitora após solicitação realizada pelo sistema;
2. O Usuário posiciona seu dedo com sua digital cadastrada na leitora após solicitação realizada pelo sistema;
3. As informações são enviadas para o sistema;
4. O Usuário informa sua senha ao sistema;
5. As informações são validadas com as informações gravadas no cartão e enviadas ao sistema principal através da Internet;
6. A informação sobre o certificado digital é enviada a Entidade Certificadora (CA) para validação e os dados são retornados ao sistema principal;
7. O Sistema principal verifica as informações e as compara com os dados armazenados no banco de dados e retorna para o Sistema se está tudo correto ou não.

Para a utilização deste mesmo processo nas autenticações internas do sistema, ou seja, as autenticações que serão realizadas durante a realização de

provas, de consultas a documentos específicos, respostas de exercícios, entre outros, é sugerido que o processo 6 descrito acima seja suprimido, sendo realizados somente os demais processos. Assim, diminui o envio de informações para a rede e agiliza o processo de autenticação do usuário.

Desta forma, o sistema não precisará ser reescrito para a utilização nas autenticações internas e terá aumentado o nível de segurança em todos os pontos do sistema onde se deseje introduzir a funcionalidade de autenticação do usuário.

4. CONCLUSÃO

O objetivo deste trabalho foi pesquisar as diversas tecnologias de cartões inteligentes e métodos biométricos existentes no mercado e disponíveis para utilização, com o intuito de analisá-las e definir um modelo que pudesse ser utilizado em um sistema de autenticação de usuários de sites de ensino à distância.

Na primeira etapa deste trabalho, focamos no estudo dos sites de EAD existentes, levantando informações de como estes sites realizavam a autenticação de seus usuários. Foi observado que a grande maioria dos sites não utiliza nenhum método de autenticação, e alguns poucos, utilizam apenas a identificação através de usuário e senha.

Foram realizadas diversas pesquisas para verificar a utilização destas duas tecnologias em conjunto para uma solução de autenticação de usuários, e concluiu-se que é viável a união das duas tecnologias, agregando a certificação digital para aumentar o nível de segurança, e que somente com esta união é que poderemos ter certeza de que uma pessoa é realmente quem diz ser.

Finalmente, uma solução foi desenhada para propor a utilização das duas tecnologias agregadas com a certificação digital para a autenticação do usuário em sites específicos de EAD.

O desenho desta solução baseou-se na utilização de um cartão inteligente com características biométricas, pois assim, poderemos realizar todas as funções de comparação do método biométrico internamente no cartão, sem haver a necessidade de extrair estas informações, o que poderia deixar uma brecha de insegurança no sistema proposto.

Na parte do método biométrico, a solução indicada é a utilização do reconhecimento digital devido as características apresentadas, principalmente a segurança e facilidade de utilização por parte do usuário. O que facilitou também

esta decisão foi encontrar produtos no mercado que já unem estas duas tecnologias em um único dispositivo.

Aliando o processo de certificados digitais à solução, foi possível verificar que o desenho ficou mais seguro e com características totalmente atualizadas.

Com o desenho da solução final, o objetivo deste trabalho foi alcançado, pois foi possível propor uma solução que integrasse as duas soluções tecnológicas, cartão inteligente e métodos biométricos e ainda agregar a certificação digital, que não estava incluída no escopo inicial do trabalho.

Como vantagens proposta pela solução final, podemos identificar:

- Maior segurança no processo de identificação do usuário em diversos pontos do sistema, visto que esta solução pode ser aplicada não somente para a autenticação inicial do usuário;
- Facilidade de utilização da solução por parte do usuário;
- Confiabilidade e confidencialidade no tratamento das informações trocadas devido a utilização de Certificação Digital;

Esta solução não apresenta desvantagens em relação ao processo de autenticação utilizado atualmente pelos sites de EAD, que foi onde este trabalho se concentrou para propor a nova solução de autenticação.

Como continuidade deste trabalho, seguem algumas sugestões que poderão ser implementadas e implantadas:

- Desenvolver a solução proposta para se ter um sistema que possa ser implantado em um site de ensino à distância;
- Verificação de soluções de cartões inteligentes e métodos biométricos que funcionem em sistemas operacionais abertos, como Linux;
- Análise de novos dispositivos biométricos para que se possam ter outras opções, além do reconhecimento digital.

REFERÊNCIAS BIBLIOGRÁFICAS

Bibliografia básica

ALVES, João Roberto Moreira. **Educação a distância e as novas tecnologias de informação e aprendizagem.** 2004. Disponível em: <http://www.engenheiro2001.org.br/programas/980201a1.htm>. Acesso em 15 jul 2003.

ANDRADE, Pedro. **A Internet e o Ensino à Distância.** 1997. Disponível em: <hppt://student.dei.uc.pt/~pandrade/sf>. Acesso em 15 jul 2003.

ASHBOURN, Julian. **Biometrics: Advanced Identity Verification – The Complete Guide.** Great Britain: Springer-Verlag, 2002.

BIODIGEST. **Biometric Digest's Biometric Information Directory.** Disponível em: <http://www.biodigest.com>. Acesso em 15 ago 2003.

CARDLOGIX Inc. **Smart Card & Security Basics.** CardLogix Inc. California: USA, 2000. Disponível em: <http:www.cardlogix.com>. Acesso em 24 jul. 2003.

CEDERJ. **Centro de Educação Superior à Distância do Estado do Rio de Janeiro**. Curso de Licenciatura em Ciências Biológicas. Disponível em http://www.cederj.edu.br/cederj/biologia/index.php. Acesso em 12 de dez de 2004.

CERTISIGN. **Primeira leitura sobre Certificação Digital.** CertiSign Inc. 2002. Disponível em: <http:www.certisign.com.br>. Acesso em 17 jul. 2003.

CHAVES, Eduardo. **Ensino à Distância: Conceitos Básicos.** 1999. Disponível em: <http://www.edutec.net/Tecnologia%20e%20Educacao/edconc.htm#Ensino%20a%20Distância>. Acesso em 15 jul 2003.

FIORESE, Maurício. **Uma solução na autenticação de usuários para ensino à distância**. Rio Grande do Sul, Universidade Federal do Rio Grande do Sul, [s.d.]. Disponível em: <http://www.inf.ufrgs.br/pos/SemanaAcademica/Semana99/fiorese/fiorese.html>.

Acesso em:10 set. 2001.

FOWLER, Martin. **UML Essencial: um breve guia para a linguagem-padrão de modelagem de dados**. Traduzido por Vera Pezerico e Christian Thomas Price. 2ª. Edição – Porto Alegre: Bookman, 2000.

HUNT, R.. **PKI and digital certification infrastructure**. Networks, 2001. Proceedings. Page(s): 234 –239. Ninth IEEE International Conference on , October 10-12, 2001.

HWANG, Min-Shiang; LI, Li-Hua. **A new remote user authentication scheme using smart cards**. Consumer Electronics, IEEE Transactions on , Volume: 46. Page(s): 28 –30. Issue: 1 , Feb. 2000.

INFINEON. **Secure - The silicon trust report**. Infineon Technologies Publication. 02/2002.

ISO 7810. **ISO Standards for Identification cards – Physical characteristics.** International Standard Organization, 1995.

ISO 7811. **ISO Standards for Identification cards – Recording technique.** International Standard Organization, 1996.

ISO 7812. **ISO Standards for Identification cards.** International Standard Organization, 1993.

ISO 7816. **ISO Standards for microcontroller Smart Cards.** International Standard Organization, 1998.

LEE, J.K.; RYU, S.R.; YOO, K.Y.. **Fingerprint-based remote user authentication scheme using smart cards**. Electronics Letters , Volume: 38. Page(s): 554 -555. Issue: 12 , 6 June 2002.

LIU, Simon; SILVERMAN, Mark. **A Practical Guide to Biometric Security Technology**. IT PRO. IEEE Computer Society. Disponível em: <http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm>. Acesso em 15 mai 2003.

MATOS, Alexandre Veloso. **UML Unified Modeling Language: Prático e Descomplicado**. São Paulo: Érica, 2002.

MIMURA, M.; ISHIDA, S.; SETO, Y. **Fingerprint verification system on smart card**. Consumer Electronics, 2002. ICCE. 2002 Digest of Technical Papers. Page(s): 182 –183. International Conference on , 18-20 June 2002.

NIST. National Institute of Standards and Technology. **Guideline for use of advanced authentication technology alternatives.** Disponível em <http://www.itl.nist.gov/fipspubs/fip190.htm>. Acesso em 13 out 2004.

PE&GN. Revista Pequenas Empresas & Grandes Negócios. **Ensino à Distância.** 2004. Disponível em: <http://empresas.globo.com/Empresasenegocios/0.19125.ERA577208-2485.00.html>. Acesso em 15 dez 2004.

PODIO, Fernando L. **Biometrics – Technologies for highly secure personal authentication.** Information Technology Laboratory – National Institute of Standards and Technology / NIST. Disponível em: <www.itl.nist.gov/lab/bulletns>. Acesso em 30 jun 2003.

RANKL, W.; EFFING, W. **Smart Card Handbook**; translated by Chanterelle Translations. England: Wiley, 1997.

RSASECURITY. **X.509 Standard.** Disponível em http://www.rsasecurity.com/rsalabs/faq/5-3-2.html. Acesso em 05 abr 2004.

SANCHEZ-REILLO, R..**Smart card information and operations using biometrics**. Aerospace and Electronic Systems Magazine, IEEE , Volume: 16 Issue: Page(s): 3 -6. 4 , April 2001.

SCHNEIER, Bruce. **Applied Cryptography Second Edition:** protocols, aogorithms, and source code in C. USA: Wiley, 1996.

STRUIF, B.; SCHEUERMANN, D.. **Smartcards with biometric user verification**. Multimedia and Expo, 2002. Proceedings. 2002 IEEE International Conference on , Volume: 2. Page(s): 589 -592 vol.2. 26-29 Aug. 2002.

THE G&D BIOMETRICS Toolkit. On-card fingersprint verification technology implemented in a tamper-proof embedded system for maximum-security user authentication. **Gieseck & Devrient,** [Alemanha], [entre 1995 e 2001].

UFMG. **Ambiente de suporte para ensino-aprendizagem à distancia.** 2004. Disponível em : http://teleduc.ead.eee.ufmg.br/pagina_inicial/index.php?. Acesso em 12 dez 2004.

UFRS. **Ensino à Distância.** 1998. Disponível em: <http://penta.ufrgs.br/~luis/Ativ1/AmbApC.html>. Acesso em 12 dez 2004.

VIGLIAZZI, Douglas. **Biometria Medidas de Segurança**. São Paulo: Visual Books, 2003.

WALDER, Bob. **Smart Cards: The use of "inteligent plastic" for access control.** England: NSS Group, 1997.

WOODWARD, John D. Jr; ORLANS, Nicholas M.; HIGGINS, Peter T., **Biometrics: Identity Assurance in the Information Age.** USA: McGraw-Hill/Osborne, 2003.

YOUNGLOVE, R.W.. **Public key infrastructure. How it works**. Computing & Control Engineering Journal , Volume: 12. Page(s): 99 –102. Issue: 2 , April 2001.

Bibliografia complementar

CHEN, Zhiqun. **Java Card Technology for Smart Cards**: architecture and programmer´s guide. California: Sun Microsystems, 2000.

CHI-KWONG CHAN; CHENG, L.M.. **Cryptanalysis of a remote user authentication scheme using smart cards**. Consumer Electronics, IEEE Transactions on , Volume: 46. Page(s): 992 –993. Issue: 4 , Nov. 2000.

CHUAH, Lee Eng. **The Future Challenges of Biometrics.** GSEC Pratical Assingnment. Version 1.4 option 1. 25 jul 2002.

HUNG-MIN SUN. **An efficient remote use authentication scheme using smart cards**. Consumer Electronics, IEEE Transactions on , Volume: 46. Page(s): 958 – 961. Issue: 4 , Nov. 2000.

LIQUN CHEN; PEARSON, S.; VAMVAKAS, A. **On enhancing biometric authentication with data protection**. Knowledge-Based Intelligent Engineering Systems and Allied Technologies, 2000. Proceedings. Fourth International Conference on , Volume: 1. Page(s): 249 -252 vol.1, 30 Aug.-1 Sept. 2000.

SANCHEZ-REILLO, R.. **Securing information and operations in a smart card through biometrics**. Security Technology, 2000. Proceedings. Page(s): 52 -55. IEEE 34th Annual 2000 International Carnahan Conference on , 23-25 Oct. 2000.

SANCHEZ-REILLO, R.; SANCHEZ-AVILA, C.. **Fingerprint verification using smart cards for access control systems**. Aerospace and Electronic Systems Magazine, IEEE , Volume: 17. Page(s): 12 -15. Issue: 9 , Sept. 2002.

SCHEUERMANN, D.. **The smartcard as a mobile security device**. Electronics & Communication Engineering Journal , Volume: 14. Page(s): 205 -210. Issue: 5 , Oct. 2002.

SCHNEIER, Bruce. **Segurança.com**: Segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001.

SMARTCARD NEWS. **Welcome to smart card**. [Alemanha], [s.d.]. Disponível em: <http://www.smartcard.co.uk>. Acesso em: 18 jul. 2003.

SUN, Hung-Min. **An efficient remote use authentication scheme using smart cards**. Departament of Computer Science and Information Engineering. 2000 IEEE Transactions on Consumer Electronics, Vol. 46, No. 46. 4 Nov.2002.

Glossário

ABS

Acrylonitrile-butadiene-styrol

Material utilizado para a fabricação do cartão plástico. Este material possui maior resistência que o padrão em PVC.

API

Application Program Interface

Um formato de mensagem, usado por um programa para comunicar-se com um outro programa que fornece serviços para ele. Por exemplo, através das APIs do Windows é possível comunicar-se com o sistema operacional para acessar alguns recursos disponibilizados por ele.

APPLET

Applets são programas projetados para ter uma execução independente dentro de alguma outra aplicação, eventualmente interagindo com esta, tipicamente, um *browser* (navegador) Web. Assim, *applets* executam no contexto de um outro programa, o qual interage com o *applet* e determina assim sua seqüência de execução

CPS

Certificate Practice Statement

É um documento que contém as práticas e atividades que uma AC implementa para emitir os certificados, É a declaração da entidade certificadora a respeito dos detalhes do seu sistema de credenciamento, e as práticas e políticas que fundamentam a emissão de certificados e outros serviços relacionados.

DES

Data Encryption Standard

É o algoritmo de criptografia mais popular. Este algoritmo atende a um padrão internacional, sendo um algoritmo simétrico que utiliza a mesma chave para

criptografar e decriptografar os dados.

EEPROM

Electrical Erasable Programmable ROM

É uma memória não volátil onde os dados e programas podem ser carregados, lidos e apagados, sob a supervisão do sistema operacional.

FRAME RELAY

Tecnologia de transmissão de dados evolutiva das redes de comutação de pacotes tipo X.25. Compartilha o meio e a banda de transmissão entre vários usuários e os pacotes são enviados ao seu destino por canais virtuais.

ISO

International Organization for Stardardization

É uma federação mundial para definição de padrões internacionais que atua em mais de 140 países.

Esta organização define padrões em diversos segmentos.

POS

Point Of Sale

Também chamado de Terminal de Ponto de Venda. É o terminal responsável pela captura e execução das transações com cartões em estabelecimentos comerciais.

PET

Polyethylene Terephthlate

È um material plástico mais conhecido como Poliéster. utilizado para a fabricação de cartões, entre outros materiais.

Este termoplástico é utilizado na produção dos Smart Cards. Sendo que podem ser trabalhados tanto em folhas como em modelagem por injeção.

PIN

Personal Identification Number

Geralmente é utilizado como referencia a senha de um usuário.

PKCS

Public-Key Cryptography Standards

São especificações desenvolvidas pelo RSA Laboratories em cooperação com desenvolvedores de segurança de todo o mundo com o propósito de acelerar o desenvolvimento da criptografia de chaves públicas. A primeira publicação foi em 1991.

PVC

PolyVinyl Chloride

É o único material plástico que não é 100% originário do petróleo. O PVC contém, em peso, 57% de cloro (derivado do cloreto de sódio - sal de cozinha) e 43% de eteno (derivado do petróleo).

RAM

Random Access Memory

É a memória em que os dados são carregados e alterados durante uma sessão. A RAM é uma memória volátil que sem energia tem seus dados apagados.

RAM

Random Access Memory

É a memória em que os dados são carregados e alterados durante uma sessão. A RAM é uma memória volátil que sem energia tem seus dados apagados.

ROM

Read-Only Memory

Um tipo de memória não volátil que é utilizada em cartões inteligentes. É utilizada principalmente para armazenar programas e dados estáticos, pois após a carga, não podem ser alterados.

RSA

Rivest, Shamir and Adleman

A sigla é a abreviação dos nomes dos seus criadores.

É o mais importante algoritmo de criptografia para chaves públicas. É muito utilizado em processos de criptografia e assinaturas digitais.

SAM

Secure Access Module

É um cartão no formato ID-1 que pode ser colocado em leitores específicos dentro dos POS e possuem as características de armazenamento de dados, geração de chaves criptográficas e processamento criptográfico.

SDLC

Synchronous Data Link Control

Este protocolo de comunicação surgiu em 1974 como parte de uma arquitetura criada pela IBM. Entre algumas de suas características, destaca-se a configuração half ou full-duplex, ponto a ponto ou multiponto.

TCP/IP

Transmission Control Protocol / Internet Protocol

Este protocolo de comunicação foi criado visando atender as necessidades de endereçamentos e interconexão de redes.

3DES ou Triple DES

O algoritmo triple-DES, que pode ser referido como 3DES, é um algoritmo modificado do algoritmo DES. Consiste em executar o algoritmo DES três vezes consecutivas, com alternativa de encriptação e decriptação. Se a mesma chave é utilizada para as três chamadas, o 3DES corresponde ao formato normal do DES, entretanto, se duas ou três chaves diferentes forem usadas, o 3DES se torna um algoritmo bem mais forte do que o algoritmo DES

ANEXOS

Anexo I - Diagrama de caso de uso

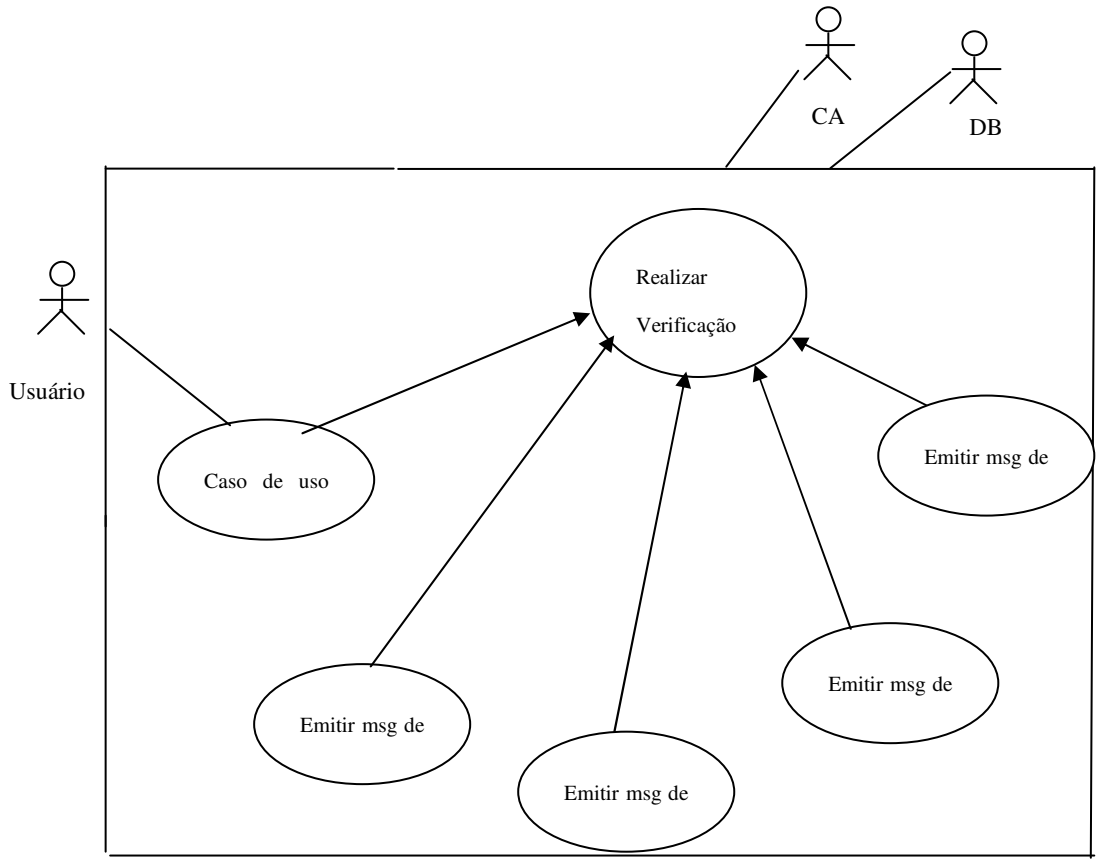


Figura 26: Diagrama de caso de uso

Anexo II - Descrição de caso de uso

Nome: Realizar verificação do usuário

Descrição: Processo de sistema em que o usuário tem suas informações verificadas pelo sistema. O usuário insere o seu cartão e sua digital na leitora, o sistema recebe estas informações e verifica junto ao DB (Banco de dados) e CA (Certificadora Digital) se as informações são válidas.

Autores:

Atores: Usuário, CA e DB

Localização: microcomputador do usuário

Posição: estágio inicial de desenvolvimento

Prioridade: 1

Suposições: Realizado sempre como parte de outro sistema.

Pré-condições: A leitora de cartões e de biometria devem estar ligadas e conectadas ao sistema.

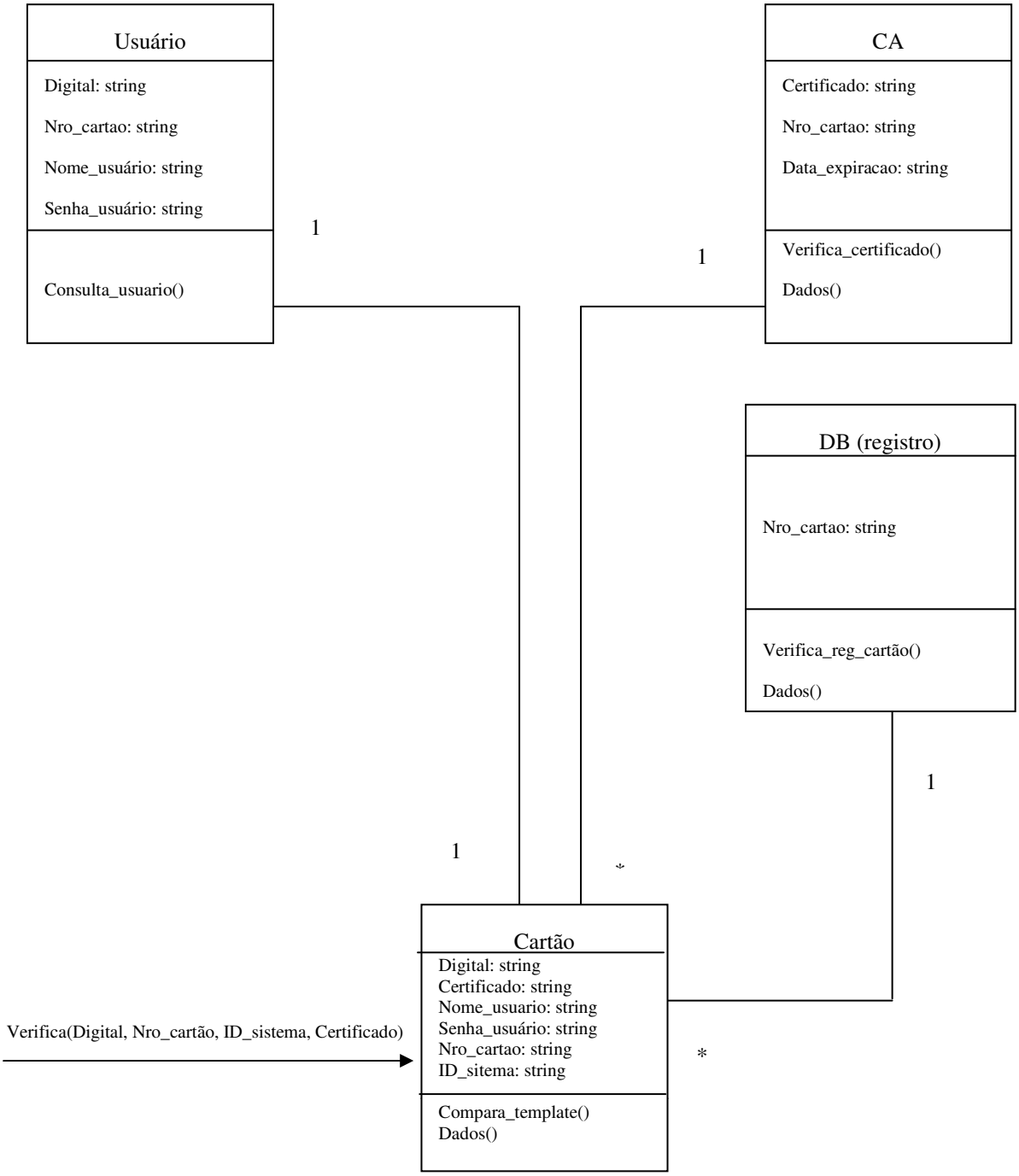
Pós-condições: Usuário validado ou negado

Caminho primário: Verificar os dados do usuário.

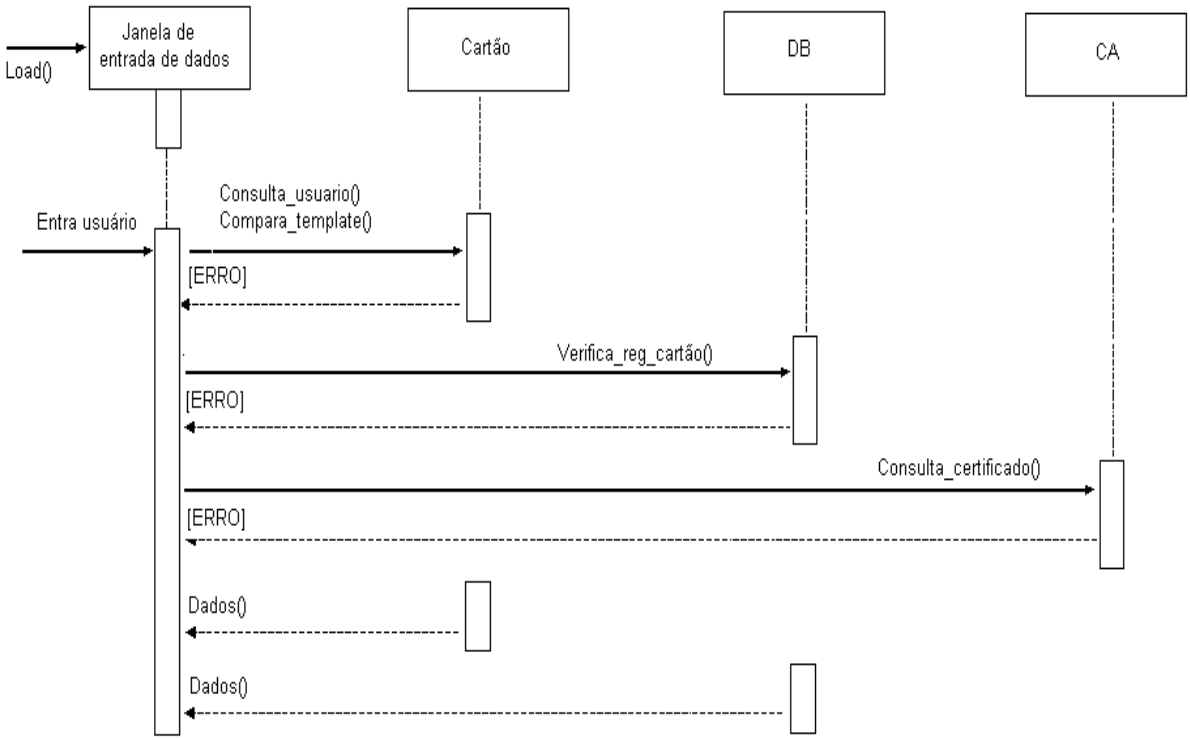
Caminho alternativo: Não há.

Caminho de exceção: Mensagens de falha de verificação das informações.

Anexo III - Diagrama de classe



Anexo IV - Diagrama de seqüência



Anexo V - Descrição da Função Principal

Função Principal()

Carrega Verifica_reg_cartao()

Se Verifica_reg_cartao(1)

Mostrar mensagem “Cartão não cadastrado no sistema”

Encerrar o programa.

Carrega Consulta_usuário()

Se Consulta_usuário(1)

Mostra mensagem “Nome não confere”

Solicita nome do usuário novamente

Se Consulta_usuário(2)

Mostra mensagem “Senha não confere”

Solicita senha novamente e acrescenta um ponto no contador de senhas erradas

Se contador for maior que o número 3

Realizar bloqueio do cartão e mostrar mensagem “Cartão bloqueado”

Encerra o programa.

Carrega Compara_template()

Se Compara_template(1)

Mostrar mensagem “Digital capturada não confere com a digital armazenada no cartão”

Solicita a inserção da digital novamente

Carrega Verifica_certificado()

Se Verifica_certificado(1)

Mostrar mensagem “Data do certificado está expirada”

Solicitar a retirada do cartão e encerrar o programa.

Se Verifica_certificado(2)

Mostrar mensagem “Certificado inválido”

Solicitar a retirada do cartão e encerrar o programa.

Libera o usuário para acessar o site desejado.

Fim de função()

Anexo VI - Descrição da Função Consulta_usuario()

Função Consulta_usuario()

Recebe dados do usuário (Nome, Senha, Número do cartão);

Verifica se o cartão está inserido na leitora;

Se o cartão não estiver inserido

Mostra mensagem "Cartão não inserido na leitora"

Envia o comando de abertura do arquivo no cartão;

Realiza a leitura dos dados do cartão (Nome, Senha, Número do cartão);

Verifica os dados recebidos com os dados armazenados no cartão;

Compara Nome recebido com Nome armazenado

Se não for igual

Retorna erro (1) na função;

Compara Senha recebida com Senha armazenada

Se não for igual

Retorna erro (2) na função;

Fim da função.

Anexo VII - Descrição da Função Verifica_certificado()

Função Verifica_certificado()

Verifica se o cartão está inserido na leitora;

Se o cartão não estiver inserido

Mostra mensagem "Cartão não inserido na leitora"

Envia o comando de abertura do arquivo no cartão;

Recebe dados do cartão (Número do cartão);

Realiza a leitura dos dados do cartão (Certificado, Data de expiração);

Verifica a Data de expiração do Certificado;

Se a Data de expiração for menor que a data do sistema

Retorna erro (1) na função;

Envia o Número do cartão e Certificado para a CA cadastrada;

A CA verifica se o Certificado é válido;

A CA retorna o resultado da verificação;

Se não estiver válido;

Retorna erro (2) na função;

Fim da função.

Anexo VIII - Descrição da Função Verifica_reg_cartao()

Função Verifica_reg_cartao()

Verifica se o cartão está inserido na leitora;

Se o cartão não estiver inserido

Mostra mensagem “Cartão não inserido na leitora”

Envia o comando de abertura do arquivo no cartão;

Realiza a leitura dos dados do cartão (Número do cartão);

Envia o comando para abertura do arquivo de cartões (DB);

Verifica se o Número do cartão está cadastrado no DB;

Se o Número do cartão não estiver cadastrado

Retorna erro (1) na função;

Fim da função.

Anexo IX - Descrição da Função Compara_template()

Função Compara_template()

Verifica se o cartão está inserido na leitora;

Se o cartão não estiver inserido

Mostra mensagem "Cartão não inserido na leitora"

Solicita ao usuário que posicione o dedo sobre a leitora;

Verifica se o dedo está posicionado;

Envia o comando de captura da digital do usuário;

Realiza a leitura dos dados do cartão (Digital armazenada);

Compara a digital capturada com a digital armazenada;

Se a Digital capturada não for igual a Digital armazenada

Retorna erro (1) na função;

Fim da função.