

FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO



FEUP

Cenários de Utilização do Cartão de Cidadão em Sistemas de Informação Académicos

André Manuel Silva Barbosa

VERSÃO FINAL

Relatório de Dissertação
Mestrado Integrado em Engenharia Informática e Computação

Orientador: Gabriel de Sousa Torcato David (Pró-Director para a Gestão de Informação)

Abril de 2010

Cenários de Utilização do Cartão de Cidadão em Sistemas de Informação Académicos

André Manuel Silva Barbosa

Relatório de Dissertação
Mestrado Integrado em Engenharia Informática e Computação

Aprovado em provas públicas pelo Júri:

Presidente: José Manuel de Magalhães Cruz (Professor Auxiliar)

Arguente: José Manuel Matos Moreira (Professor Auxiliar)

26 de Março de 2010

Resumo

A autenticação dos utilizadores é um requisito essencial para permitir oferecer interacções diferenciadas e sofisticadas com sistemas de informação. Essa autenticação de utilizadores pela primeira vez ou ocasionais tem sido tratada de diversas formas, a maior parte com óbvias fragilidades. Pretende-se neste trabalho estudar as possibilidades abertas pelas funcionalidades de autenticação previstas no Cartão de Cidadão, e implementar API's de suporte às mesmas, facilmente integráveis com sistemas de autorização em sistemas de informação na web.

O Cartão de Cidadão, o novo documento de cidadania, é um projecto dinamizador da modernização da Administração Pública em Portugal que visa a melhoria das relações entre o cidadão e o Estado. É um documento que, na sua componente física e visual, substitui o bilhete de identidade, o cartão de contribuinte, o cartão de membro da Segurança Social, o cartão de utente do Serviço Nacional de Saúde e cartão de eleitor. Na sua vertente digital, promove o desenvolvimento das transacções electrónicas através de mecanismos de forte segurança na autenticação e da introdução de assinaturas digitais qualificadas do cidadão.

É neste contexto que a Universidade do Porto e a Faculdade de Engenharia em particular, pretendem integrar no SI existente, funcionalidades de segurança avançada com recurso às tecnologias associadas ao Cartão de Cidadão. Para que estes mecanismos sejam implementados com sucesso, foram analisadas as melhores propostas e cenários de utilização do cartão enquanto documento electrónico, quais as suas potencialidades e limitações na integração com sistemas existentes do uso dos certificados de autenticação e assinatura digital.

Ligeiramente fora do âmbito da dissertação, mas com um impacto na implementação a ter em conta, surge a encriptação de dados através das estruturas de certificados digitais suportadas pelo Cartão de Cidadão directa ou indirectamente através de uma camada intermédia. Estes cenários de utilização são especialmente interessantes nos dias de hoje pela desconfiança cada vez maior das pessoas em relação aos sistemas de armazenamento de dados, porque apesar da existência de mecanismos de autenticação mais ou menos seguros e da possibilidade de definir permissões de acesso a determinados conteúdos, os administradores da base de dados continuam a ter a possibilidade de visualizar essa informação, através de uma camada de acesso de baixo nível, que ignora todas as restrições da lógica de negócio de uma aplicação. Para combater este fenómeno apresentamos uma abordagem à encriptação da informação armazenada na base de dados, que pretende assegurar aos utilizadores que mais ninguém consegue visualizar informações por eles definidas.

Assim, os objectivos principais da dissertação passam não só pela configuração e desenho de uma estrutura de suporte à integração do SI com o Cartão de Cidadão nas áreas de segurança que foram apresentadas acima, mas também pela criação de diversos métodos de acesso a dados armazenados no cartão. É um projecto bastante inovador na medida em que confere ao sistema a ser munido com estas funcionalidades a adaptação a todo um novo paradigma de controlo de acessos, validação de identidades e integridade dos dados armazenados.

Abstract

Users authentication is an essential requirement to allow differentiated and sophisticated interactions with information systems. The users authentication for the first time or at randomly has been treated in many ways, most of them with obvious fragilities. It is expected during this project to analyse the possibilities opened by the authentication features made available in the Portuguese Citizen Card, and implement API's for supporting them, than can easily be integrated with authorization systems inside information systems on the web.

The Portuguese Citizen Card, the new citizenship document, is a modernization promoter project from the Public Administration in Portugal that aims the improvement of the relations between the citizen and the State. Regarding the physical and visual component, the document replaces the identification card, the taxes contribution card, the National Insurance member card, the National Health Service user card and the voter card. As a digital component, promotes the development of electronic transactions through strong security mechanisms involved in the authentication process and the introduction of qualified digital signatures from the citizen.

These are the concepts University of Porto and the Faculty the Engineering in particular, would like to integrate with the existent IS, advanced security features using the technologies connected with the Portuguese Citizen Card. In order for these mechanisms to be successfully implemented, the best proposals and usage scenarios for the card as an electronic document were analysed, like which are the abilities and limitations of integrating existing systems with the usage of its digital certificates for authentication and digital signature.

Slightly outside the scope of the dissertation, but with an impact on the implementation to be taken into account, arises the data encryption through the digital certificates structures supported by the Portuguese Citizen Card direct or indirectly through an intermediate layer. The usage scenarios are very interesting nowadays due to the increasing distrust from the persons regarding data storage systems, because even if there are authentication mechanisms more or less secure and the possibility to define access permissions to different contents, the database administrators still have the possibility to see this information, through a low level access layer, that ignores all the business rules restrictions of an application. To fight this phenomenon we present an approach to the encryption of the information stored in the database, that aims to assure the users that no one else can see data defined by them.

So, the main goals of the dissertation are not only the configuration and design of a support structure for the IS integration with the Portuguese Citizen Card in the security areas presented above, but also the creation of several access methods to the data stored in the card. The project itself is very innovative and completes the systems where these feature will be added with the adaption to a new paradigm of accesses control, identities validation and integrity of data stored.

Agradecimentos

Ao meu orientador, o Prof. Gabriel David, pela disponibilidade, dedicação, encorajamento e conselhos recebidos de maneira a que o objectivo em vista fosse possível.

Ao meu co-orientador, o Eng. Manuel Machado, pela oportunidade que me foi dada e pelo acompanhamento construtivo.

Aos meus colegas de trabalho Helder Maia e Hugo Zenha, pela ajuda e conselhos que me foram dados ao longo do projecto.

A alguns elementos do ITIJ e do MJ pelos esclarecimentos prestados, assim como a alguns elementos da CNPD pelo mesmo feito.

À minha família, pelo apoio e suporte neste período de mudança e à minha irmã em especial pela ajuda prestada a todos os níveis.

À minha noiva Ania, que tornou possível a nossa presença em Portugal e que me garantiu o equilíbrio indispensável ao longo deste meu percurso, ao qual ficará ligada para sempre.

André Barbosa

Abril de 2010

Índice

1	Introdução.....	1
1.1	Contexto.....	1
1.2	Enquadramento.....	1
1.2.1	CICA.....	2
1.2.2	Sysnovare.....	2
1.3	Motivação.....	2
1.4	Objectivos.....	3
1.5	Página da Dissertação.....	3
1.6	Estrutura da Dissertação.....	4
2	Estado da Arte.....	5
2.1	Introdução.....	5
2.2	Enquadramento Tecnológico.....	5
2.2.1	SIGARRA.....	6
2.2.2	GESSI.....	7
2.2.3	GP.....	7
2.2.4	Ferramentas Externas.....	8
2.2.4.1	Eclipse.....	8
2.2.4.2	Google Code.....	8
2.3	Criptografia.....	8
2.3.1	Encriptação e Desencriptação.....	9
2.3.1.1	Encriptação Simétrica.....	9
2.3.1.2	Encriptação Assimétrica.....	10
2.3.2	Assinaturas Digitais.....	11
2.3.2.1	Algoritmos de Dispersão.....	12
2.3.2.2	Selos Temporais.....	13
2.3.2.3	Legislação.....	14
2.3.3	Certificados Digitais.....	14
2.3.3.1	Autoridades de Certificação.....	16
2.3.3.2	Infra-estruturas de Chaves Públicas.....	16
2.3.3.3	Listas de Revogação de Certificados.....	17
2.4	Cartão de Cidadão.....	17
2.4.1	Objectivos.....	17
2.4.2	Características.....	18

2.4.3	Entidades de Certificação.....	19
2.4.3.1	SCEE.....	20
2.4.3.2	Hierarquia.....	20
2.4.4	Casos de Estudo.....	21
2.4.4.1	SAPO.....	21
2.4.4.2	IST.....	22
2.5	Java.....	22
2.5.1	iText.....	23
2.5.2	eID Applet.....	23
2.6	Oracle.....	23
2.6.1	Segurança Avançada.....	24
2.6.1.1	Encriptação Transparente de Dados.....	24
2.7	Resumo.....	25
3	Descrição do Problema.....	27
3.1	Introdução.....	27
3.2	Cenários de Utilização.....	27
3.2.1	Autenticação.....	28
3.2.1.1	Autenticação de Utilizadores.....	28
3.2.1.2	Identificação de Pessoas Externas.....	29
3.2.1.3	Recuperação da Senha de Acesso.....	30
3.2.1.4	Preenchimento Automático de Formulários.....	31
3.2.1.5	Controlo de Acessos.....	33
3.2.1.6	Controlo da Assiduidade.....	34
3.2.2	Assinatura Digital.....	35
3.2.2.1	Assinatura de Documentos.....	35
3.2.2.2	Assinatura de Mensagens Electrónicas.....	36
3.2.2.3	Assinatura de Conteúdos da Base de Dados.....	37
3.2.3	Encriptação.....	38
3.2.3.1	Encriptação de Documentos.....	38
3.2.3.2	Encriptação de Mensagens Electrónicas.....	39
3.2.3.3	Encriptação de Conteúdos da Base de Dados.....	40
3.3	Resumo.....	41
4	Solução Proposta.....	43
4.1	Introdução.....	43
4.2	Autenticação.....	44
4.2.1	Autenticação de Utilizadores.....	44
4.2.1.1	Requisitos.....	45
4.2.1.2	Estrutura de Dados.....	45
4.2.1.3	Modo de Funcionamento.....	46
4.2.2	Identificação de Pessoas Externas.....	47
4.2.2.1	Requisitos.....	47
4.2.2.2	Estrutura de Dados.....	47
4.2.2.3	Modo de Funcionamento.....	47
4.2.3	Recuperação da Senha de Acesso.....	47

4.2.3.1	Requisitos.....	48
4.2.3.2	Estrutura de Dados.....	48
4.2.3.3	Modo de Funcionamento.....	48
4.2.4	Preenchimento Automático de Formulários.....	48
4.2.4.1	Requisitos.....	48
4.2.4.2	Estrutura de Dados.....	49
4.2.4.3	Modo de Funcionamento.....	49
4.2.5	Controlo de Acessos.....	50
4.2.6	Controlo da Assiduidade.....	50
4.3	Assinatura Digital.....	50
4.3.1	Assinatura de Documentos.....	50
4.3.1.1	Requisitos.....	51
4.3.1.2	Estrutura de Dados.....	51
4.3.1.3	Modo de Funcionamento.....	51
4.3.2	Assinatura de Mensagens Electrónicas.....	51
4.3.2.1	Requisitos.....	52
4.3.2.2	Estrutura de Dados.....	52
4.3.2.3	Modo de Funcionamento.....	52
4.3.3	Assinatura de Conteúdos da Base de Dados.....	52
4.3.3.1	Requisitos.....	53
4.3.3.2	Estrutura de Dados.....	53
4.3.3.3	Modo de Funcionamento.....	54
4.4	Encriptação.....	55
4.4.1	Encriptação de Documentos.....	55
4.4.1.1	Requisitos.....	55
4.4.1.2	Estrutura de Dados.....	56
4.4.1.3	Modo de Funcionamento.....	56
4.4.2	Encriptação de Mensagens Electrónicas.....	57
4.4.2.1	Requisitos.....	57
4.4.2.2	Estrutura de Dados.....	57
4.4.2.3	Modo de Funcionamento.....	57
4.4.3	Encriptação de Conteúdos da Base de Dados.....	58
4.4.3.1	Requisitos.....	58
4.4.3.2	Estrutura de Dados.....	58
4.4.3.3	Modo de Funcionamento.....	59
4.5	Biblioteca de Software para o Cartão de Cidadão.....	60
4.6	Arquitectura.....	60
4.6.1	Divisão Funcional.....	60
4.6.2	Lógica de Negócio.....	61
4.7	Resumo.....	62
5	Implementação.....	65
5.1	Introdução.....	65
5.2	Nomenclaturas.....	65
5.2.1	Java.....	66

5.2.2 PL/SQL.....	66
5.3 MSA.....	67
5.4 PTEID4J.....	67
5.5 Autenticação.....	67
5.5.1 Configurações.....	67
5.5.2 Demonstração.....	68
5.6 Resumo.....	71
6 Conclusões e Trabalho Futuro.....	73
6.1 Satisfação dos Objectivos.....	73
6.2 Trabalho Futuro.....	73
Referências.....	75
Índice Remissivo.....	87

Lista de Figuras

Figura 2.1: Arquitectura Física das aplicações GESSI e SIGARRA.....	6
Figura 2.2: Google Code.....	8
Figura 2.3: Encriptação e Desencriptação.....	9
Figura 2.4: Encriptação Simétrica.....	10
Figura 2.5: Encriptação Assimétrica.....	11
Figura 2.6: Diagrama dos processos de Assinatura Digital e Verificação da mesma.....	12
Figura 2.7: Diagrama Exemplo do uso de Algoritmos de Dispersão.....	13
Figura 2.8: Diagrama de Inserção de um Selo Temporal num Documento.....	14
Figura 2.9: Ilustração da finalidade de um Certificado Digital.....	15
Figura 2.10: Ataque do Homem no Meio.....	15
Figura 2.11: Diagrama de uma Infra-estrutura de Chaves Públicas.....	16
Figura 2.12: Logotipo do Cartão de Cidadão.....	17
Figura 2.13: Aspecto Físico do Cartão de Cidadão.....	19
Figura 2.14: Hierarquia das Entidades de Certificação do Cartão de Cidadão.....	20
Figura 2.15: Autenticação no SAPO com Cartão de Cidadão.....	21
Figura 2.16: Autenticação no IST com o Cartão de Cidadão.....	22
Figura 2.17: Logotipo do Java.....	22
Figura 2.18: Logotipo do iText.....	23
Figura 2.19: Logotipo da Oracle.....	24
Figura 2.20: Diagrama de Funcionamento da Segurança Avançada da Oracle.....	24
Figura 2.21: Diagrama da Encriptação Transparente de Dados da Oracle.....	25
Figura 4.1: Logotipo do Apache.....	44
Figura 4.2: Estrutura de Dados para a Autenticação de Utilizadores.....	46
Figura 4.3: Estrutura de Dados para a detecção automática de dados do Cartão de Cidadão.....	49
Figura 4.4: Estrutura de Dados para a Assinatura de Colunas na Base de Dados.....	53
Figura 4.5: Estrutura de Dados para a Assinatura de Registos na Base de Dados.....	54
Figura 4.6: Estrutura de Dados para a Encriptação de Documentos.....	56
Figura 4.7: Estrutura de Dados para a Encriptação de Mensagens Electrónicas.....	57
Figura 4.8: Estrutura de Dados para a Encriptação de Conteúdos da Base de Dados.....	59
Figura 4.9: Divisão Funcional da Arquitectura da Solução Proposta.....	61
Figura 4.10: Lógica de Negócio da Arquitectura da Solução Proposta.....	62
Figura 5.1: Configurações do Apache para a Autenticação com o Cartão de Cidadão.....	68
Figura 5.2: Demonstração da Autenticação com o Cartão de Cidadão.....	69
Figura 5.3: Demonstração do pedido do Certificado de Autenticação do Cartão de Cidadão.....	69
Figura 5.4: Demonstração do pedido de PIN de Autenticação do Cartão de Cidadão.....	70

Lista de Tabelas

Tabela 5.1: Sufixos dos Pacotes em PL/SQL.....	66
Tabela 5.2: Parâmetros SSL enviados do Cliente para o Servidor.....	71

Abreviaturas e Símbolos

AC	Autoridade de Certificação (versão portuguesa de CA)
AMA	Agência para a Modernização Administrativa
APDU	Application Protocol Data Unit
API	Application Programming Interface
BD	Base de Dados (versão portuguesa de DB)
BI	Bilhete de Identidade
CA	Certificate Authority
CC	Cartão de Cidadão
CEO	Chief Executive Officer
CICA	Centro de Informática Prof. Correia Araújo
CNPD	Comissão Nacional de Protecção de Dados
CRL	Certificate Revocation List
CSS	Cascade Style Sheet
DB	DataBase
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EC	Entidade Certificadora ou Entidade de Certificação (versão portuguesa de CA)
eID	electronic IDentification
FEUP	Faculdade de Engenharia da Universidade do Porto
GESSI	GEStão do Sistema de Informação
GP	Gestão de Projectos
HTTP(S)	Hyper Text Transfer Protocol (Secure)
ICP	Infra-estrutura de Chaves Públicas (versão portuguesa de PKI)
IDE	Integrated Development Environment
IIS	Internet Information Services
IRN	Instituto dos Registos e do Notariado
IT	Information Technology
ITIJ	Instituto das Tecnologias de Informação na Justiça
JS	JavaScript

OAS	Oracle Advanced Security
OCF	Open Card Framework
OCSP	Online Certificate Status Protocol
MSA	Módulo de Segurança Avançada
MIEIC	Mestrado Integrado em Engenharia Informática e Computação
MITM	Man-In-The-Middle (attack)
MJ	Ministério da Justiça
NIC	Número de Identificação Civil
NIF	Número de Identificação Fiscal
OAS	Oracle Advanced Security
PDF	Portable Document Format
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PSI	Projecto de Sistemas de Informação
RSA	Rivest, Shamir and Adleman
SC	Smart Card
SCEE	Sistema de Certificação Electrónica do Estado
SI	Sistema de Informação
SIGARRA	Sistema de Informação para a Gestão Agregada de Recursos e dos Registos Académicos
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SSL	Secure Socket Layer
SSO	Single Sign-On
TI	Tecnologia da Informação (versão portuguesa de IT)
TLS	Transport Layer Security
TTP	Trusted Third Party
TTS	Trusted TimeStamping
TSA	TimeStamping Authority
UML	Unified Modelling Language
UP	Universidade do Porto
W3C	World Wide Web Consortium
XAdES	XML Advanced Electronic Signatures
XML	eXtensible Markup Language

1 Introdução

A autenticação dos utilizadores é um requisito essencial para permitir oferecer interacções diferenciadas e sofisticadas com sistemas de informação. A autenticação de utilizadores pela primeira vez ou ocasionais tem sido tratada de diversas formas, a maior parte com óbvias fragilidades. Pretende-se neste trabalho estudar as possibilidades abertas pelas funcionalidades de autenticação previstas no Cartão de Cidadão e implementar API's de suporte às mesmas, facilmente integráveis com mecanismos de autorização em sistemas de informação na web.

1.1 Contexto

Esta dissertação faz parte do plano de estudos para a obtenção do Mestrado Integrado em Engenharia Informática e computação (MIEIC) na Faculdade de Engenharia da Universidade do Porto (FEUP). É a última fase de um longo percurso que transforma um estudante universitário num cidadão com potencial para encarar o mundo empresarial ou de prosseguir uma carreira na investigação e/ou ensino. Acima de tudo, pretende-se que o aluno obtenha experiência laboral numa instituição externa à faculdade e que o seu projecto retorne algo de inovador inserido obviamente no âmbito do mestrado em questão.

1.2 Enquadramento

As possibilidades de utilização do Cartão de Cidadão estão agora a ser concretizadas e é especialmente inovador o estudo dos cenários de utilização em contexto universitário. Este é o caminho que a Universidade do Porto (UP) pretende seguir no sentido de completar o seu sistema de informação, o SIGARRA, com mecanismos de segurança ainda mais inovadores. É com este intuito que surge a possibilidade da realização deste projecto através de uma parceria entre a FEUP e a Sysnovare com vantagens para ambos: a FEUP pelas razões descritas acima e a Sysnovare porque passa a contar com mais funcionalidades nas suas aplicações e talvez maior competitividade no mercado das Tecnologias da Informação (TI's).

1.2.1 CICA

O Centro de Informática Prof. Correia de Araújo (CICA) é um serviço central da FEUP e a sua missão é disponibilizar e assegurar a operacionalidade de recursos e serviços de informática para toda a comunidade da faculdade, promovendo a sua utilização e inovação. Actualmente o CICA emprega cerca de 60 pessoas e está dividido em quatro unidades funcionais: Unidade de Administração de Sistemas (UAS), Unidade de Infra-Estruturas e Redes de Comunicação (UIRC), Unidade de Microinformática e Suporte ao Utilizador (UMSU) e Unidade de Sistemas de Informação (USINF) [CICA01, CICA02].

Através de uma equipa designada por Projecto de Sistemas de Informação (PSI), o CICA é também responsável, em conjunto com uma equipa técnica da reitoria, a Universidade Digital, e outra da Faculdade de Ciências, pelo desenvolvimento e manutenção do SIGARRA. Foi com os elementos desta equipa que a maioria dos contactos foram estabelecidos no sentido de obter conhecimento do sistema existente e ponderar decisões a tomar relativamente à alteração da arquitectura do mesmo inerentes à implementação das novas funcionalidades visadas na dissertação.

1.2.2 Sysnovare

A Sysnovare surgiu em Abril de 2009 para dar resposta aos novos desafios das TI's e às cada vez mais frequentes exigências dos clientes de aplicações desta área. A sua criação está em muito ligada às possibilidades de expansão dos produtos desenvolvidos na FEUP para outros mercados e com outras responsabilidades que não as do universo da UP [SYNV01]. A ligação entre as duas instituições está ainda bem patente, não só pela troca de conhecimento que existe entre ambas mas também pelo passado e presente em comum.

Neste momento a empresa conta com cerca de 20 colaboradores, na sua maioria pessoas ligadas ao desenvolvimento das aplicações disponibilizadas e tudo o que está inerentemente associado a esta actividade. Foi neste ambiente que fisicamente o projecto decorreu, mas nunca deixou de haver troca de informação e entendimento entre ambas as instituições.

1.3 Motivação

As oportunidades que podem surgir com a introdução do Cartão de Cidadão na sociedade portuguesa, principalmente no campo tecnológico, são enormes e potenciam o aumento e o sucesso das relações dos cidadãos tanto com os organismos do Estado como com as entidades privadas. Quem nunca se queixou do excesso de burocracia ou do elevado tempo de espera quando interagiu de algum forma com o Governo?

É esta imagem que as pessoas têm de Portugal que o plano tecnológico, e neste caso em concreto o Cartão de Cidadão, pretende de certa forma limpar da cabeça dos portugueses através da introdução de medidas inovadoras e tecnologicamente audazes capazes de transmitir à população um sentimento de confiança no sistema [CCOB01]. E mais do que ver esta mudança acontecer é sem dúvida motivador poder fazer parte dela e contribuir para que a Universidade do Porto, enquanto instituição pública e portadora de uma considerável reputação tanto a nível nacional como internacional, esteja na linha da frente no que diz respeito à inovação nas metodologias de interacção com os seus utilizadores, na sua grande maioria cidadãos de Portugal.

1.4 Objectivos

Tal como foi mencionado acima, as potencialidades que o Cartão de Cidadão oferece são imensas, mas o mesmo não acontece com o tempo e recursos disponíveis para a dissertação. E tendo em conta essas limitações é necessário separar bem aqueles que são os objectivos a atingir dentro do prazo dos que se devem deixar em aberto para desenvolvimento futuro. A necessidade mais imediata está associada à utilização efectiva do Cartão de Cidadão no SI, sendo que todas as questões não ligadas directamente ao cartão devem ser analisadas em segundo plano, sem plano de desenvolvimento concreto. Assim, os objectivos da dissertação passam por estudar os mecanismos de autenticação suportados pelo Cartão de Cidadão em particular nas seguintes vertentes:

- Hardware e drivers necessários;
- Identificação/autenticação de utilizadores registados no sistema;
- Identificação/autenticação de utilizadores novos, passwords one-shot;
- Confirmação da identidade em actos especialmente críticos no SI;
- Assinatura digital de documentos externos ao SI;
- Encriptação interna e externa de documentos;
- Definição de cenários de utilização das várias funcionalidades;
- Implementação de APIs de configuração amigável e que não exijam grandes investimentos na reformulação de SI's existentes.

1.5 Página da Dissertação

Um dos aspectos a realçar após uma primeira fase de investigação sobre a utilização do Cartão do Cidadão, tanto a nível de configuração dos servidores para permitir a autenticação dos utilizadores como a sua utilização a nível pessoal, é a falta de informação disponível para uso com diversos sistemas operativos e aplicações. Se é verdade que a informação disponibilizada pela Agência para a Modernização Administrativa (AMA) no portal do Cartão de Cidadão está relativamente bem estruturada e apresenta manuais de utilização bastante completos para o uso do cartão naquele que é um ambiente Microsoft (Windows, Office, IIS, ...), também é verdade que comparativamente com outros países analisados há uma lacuna de informação equivalente para a utilização multi-plataforma [CCMN01]. Este pormenor tem bastante impacto no desenrolar da dissertação não só porque como vamos perceber mais à frente a FEUP não utiliza o ambiente descrito acima a nível de suporte aplicacional mas também porque cada vez mais as pessoas, e neste caso em concreto, os cidadãos portugueses têm o direito de optar pela aplicação que querem utilizar, sobretudo se a que é recomendada é também proprietária. Sobre os poucos exemplos encontrados com uma implementação semelhante à analisada nesta dissertação não existe nenhuma documentação associada, como é o caso do novo sistema de autenticação do portal SAPO, que apesar de disponibilizar um repositório de software livre, não apresenta nenhum tipo de documentação associado à implementação desse mesmo mecanismo [SPLG01, SPSL01].

Para colmatar esta falta de informação e também para servir de manual para outras pessoas ligadas à área de desenvolvimento ou arquitectura de aplicações informáticas, foi criada uma página web associada à dissertação, disponível na Internet e sem restrições de acesso. O maior objectivo da página passa pela disponibilização de manuais de configuração e utilização para ferramentas e aplicações para a integração com o Cartão de Cidadão e também de alguns conteúdos discutidos aqui na dissertação. Apesar de não ser uma prática comum neste tipo de

Introdução

projecto a abertura da informação analisada, na maior parte dos casos porque esta é confidencial à instituição que acolhe o estudante, achamos mais importante contribuir de alguma forma para a aproximação aos outros países neste aspecto e para uma maior uniformização da utilização do cartão a nível nacional.

1.6 Estrutura da Dissertação

Para além da introdução, esta dissertação contém mais 5 capítulos. No capítulo 2, é descrito o estado da arte, é feita uma introdução às tecnologias envolvidas no desenrolar do projecto e são apresentados trabalhos relacionados. No capítulo 3, é feita uma descrição completa do problema da utilização do Cartão de Cidadão em sistemas de informação académicos e quais os cenários que se pretende analisar com mais ou menos prioridade atendendo às vantagens que cada um representa contra os seus custos de implementação. No capítulo 4, são apresentadas possíveis soluções para os problemas descritos no capítulo anterior e quais as decisões tomadas para a sua implementação. No capítulo 5, é possível observar de um ponto de vista mais técnico como é que as soluções descritas foram implementadas, entre passos de configuração, código de implementação e outros aspectos da arquitectura da solução. No último capítulo da dissertação, o capítulo 6, são apresentadas as conclusões finais relativamente ao trabalho desenvolvido no decorrer do projecto e quais as perspectivas de desenvolvimento futuro, sobre aquele que se pretende que seja um grande elemento de interacção entre as pessoas e as instituições públicas e/ou privadas, o Cartão de Cidadão.

2 Estado da Arte

Neste capítulo é descrito o levantamento do estado da arte das tecnologias associadas à utilização do Cartão de Cidadão para efeitos de autenticação, assinatura digital e encriptação. O capítulo começa com uma análise tecnológica do sistema actual e avança depois para secções específicas a cada uma das áreas técnicas envolvidas no projecto, desde as componentes da criptografia até às várias questões do próprio cartão. São ainda estabelecidas comparações com outros países no uso do cartão de cidadania de cada um e são também mostrados alguns exemplos de utilização do CC em Portugal.

2.1 Introdução

Devido ao grande número de tecnologias envolvidas no projecto é de esperar que este capítulo seja composto por um número considerável de páginas, tendo em conta que é muito importante perceber e compreender todos os mecanismos associados ao uso do Cartão de Cidadão, não só do ponto de vista técnico mas também do ponto de vista legal. Assim, desde descrição de áreas concretas da criptografia, algoritmos de encriptação utilizados, limitações e restrições impostas até à arquitectura do cartão, vão ser apresentados de forma detalhada muitos campos de estudo em áreas distintas.

2.2 Enquadramento Tecnológico

Antes de avançarmos no estado da arte, para os conteúdos que transmitem inovação e que justificam a existência desta dissertação, é importante percebermos o tipo de sistema em que esta se enquadra, isto é, quais são as tecnologias associadas ao sistema existente e quais as suas limitações e potencialidades a nível de interoperabilidade com outras aplicações ou plataformas. Assim, nesta secção, será feita uma apresentação não só a nível teórico mas também a nível técnico das aplicações sobre as quais o projecto será analisado e implementado, nomeadamente do GESSI e do SIGARRA.

Ambas as aplicações correm sobre uma base de dados Oracle 10g (prevista migração para a versão 11g em breve) que dispõe também de um servidor web (Apache) que recebe os pedidos HTTP(S) dirigidos ao sistema e no caso de serem pedidos que impliquem acessos a

procedimentos PL/SQL, são passados ao servidor da base de dados que executa o código e passa o resultado do mesmo novamente ao servidor web que, por sua vez, o passa ao utilizador através de um navegador web (browser). Além de código PL/SQL, o servidor tem também a capacidade de executar código Java, previamente armazenados na base de dados, através da máquina virtual Java incorporada. A figura 2.1 mostra a arquitectura física das aplicações em questão.

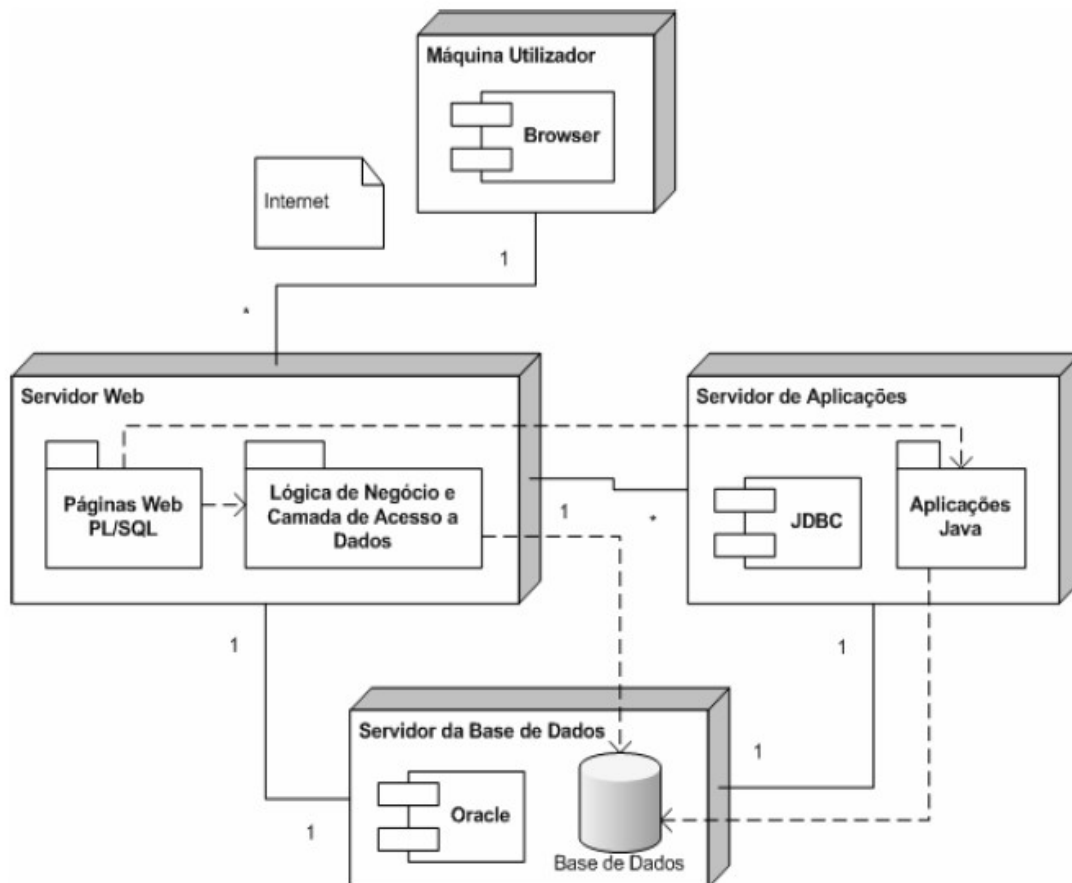


Figura 2.1: Arquitectura Física das aplicações GESSI e SIGARRA

2.2.1 SIGARRA

O Sistema de Informação para a Gestão Agregada dos Recursos e dos Registos Académicos da Universidade do Porto (SIGARRA), como o nome indica, é o sistema utilizado no apoio ao funcionamento e gestão das várias unidades orgânicas da UP, permitindo a consolidação de informação ao nível da universidade. É simultaneamente um sistema que disponibiliza serviços, através da difusão dos recursos informativos da UP, da disponibilização de diversas funcionalidades aos seus utilizadores e da facilitação da colaboração interna e externa e uma infra-estrutura, servindo de espinha dorsal ao desenvolvimento de aplicações.

A primeira versão do SIGARRA foi desenvolvida na FEUP, em 1996, tomando então o nome do SI da faculdade, o SIFEUP. O sucesso do projecto, corroborado por prémios ganhos a nível nacional e internacional, levou a UP a acordar com a FEUP o licenciamento do SIFEUP para as restantes instituições da universidade, tomando então a sua corrente designação. Actualmente, o SIGARRA é utilizado por todas as unidades orgânicas que constituem a UP [UPSG01, UPSG02].

O SIGARRA interrelaciona-se com o sistema de Gestão de Alunos da Universidade do Porto (GAUP), criado em 1992, com o objectivo de fornecer uma plataforma de gestão de dados dos alunos nas secretarias das faculdades, e com o sistema de Gestão de Recursos Humanos da Universidade do Porto (GRHUP), criado em 2000, com o objectivo de ser uma aplicação centralizada para uso do serviço de pessoal da UP. Ambos os sistemas são disponibilizados para todas as instituições da UP e a sua ligação com a SIGARRA pode ser vista na figura .

2.2.2 GESSI

A aplicação de Gestão do Sistema de Informação (GESSI) é responsável pelo suporte do SIGARRA no que diz respeito à autenticação, gestão de utilizadores, permissões de acesso às diferentes páginas e muitos outros aspectos ligados à administração do sistema principal. Apesar de a sua origem estar muito ligada ao SIGARRA, o GESSI pode suportar a administração de outros SI's graças à flexibilidade com que foi arquitectado. É uma ferramenta de eleição na Sysnovare que faz uso em pleno das suas potencialidades para a gestão de diversas aplicações.

O GESSI está conceptualmente dividido em duas grandes componentes: uma área de configurações onde estão definidos ficheiros CSS, ficheiros JS, páginas estáticas, grupos de utilizadores, permissões de acesso às páginas, domínios e imagens e outra área que diz respeito à visualização do conteúdo das páginas propriamente dito, isto é, com base nas configurações descritas anteriormente, o GESSI é capaz de gerar dinamicamente o conteúdo de uma página, automaticamente validar o acesso a esta e, em caso de sucesso, mostrar todas as componentes que a constituem.

2.2.3 GP

Além do SIGARRA e do GESSI, as duas principais aplicações associadas ao projecto, importa também referir a ferramenta de Gestão de Projectos (GP) da FEUP que serve de apoio ao desenvolvimento à equipa do PSI no CICA e à equipa técnica da Sysnovare. Tal como as duas aplicações descritas acima, é baseada numa base de dados Oracle com geração de páginas web para visualização da informação. É uma aplicação de gestão de projectos bastante orientada ao tipo de desenvolvimento que é feito na FEUP, onde as potencialidades saltam à vista na utilização com objectos Oracle e código PL/SQL, mas que pode ser usada para fazer a gestão de qualquer outro tipo de ficheiros, abdicando, como é óbvio, de muitas funcionalidades.

Entre outras coisas, esta ferramenta permite a criação de projectos, criação de módulos para um projecto, introdução dos requisitos para um módulo, criação de problemas (tarefas) e associação a outros elementos da equipa e a elaboração de casos de teste para validação dos requisitos previamente definidos. Na aplicação está incorporado um mecanismo de controlo de versões de objectos automático, o que hoje em dia é uma funcionalidade essencial em qualquer ambiente de desenvolvimento e facilita imenso o trabalho no retrocesso de código para a resolução de problemas mais complexos. Faz parte da aplicação também uma componente de

planeamento que permite fazer uma melhor gestão do tempo gasto na resolução de um problema ou tarefa e permite também um melhor controlo das datas de entrega associadas a um projecto, o que transmite uma organização do trabalho muito mais estruturada.

2.2.4 Ferramentas Externas

Não sendo efectivamente um ponto de análise tecnológica no verdadeiro sentido da palavra a escolha de ferramentas a utilizar ao longo de um projecto é sem dúvida importante e pode afectar o trabalho realizado. Assim, nesta secção será feita uma apresentação das ferramentas que foram utilizadas para o desenvolvimento do módulo para a integração do SIGARRA com o Cartão de Cidadão.

2.2.4.1 Eclipse

O Eclipse é IDE para desenvolvimento multi-linguagem com um sistema de extensões de grande qualidade. É um dos ambientes de edição de código mais utilizado no mundo e a sua componente de desenvolvimento de Java, a linguagem inicial, é muito boa. Esta ferramenta foi utilizada para o código implementada em Java no âmbito do projecto.

2.2.4.2 Google Code

O Google Code é uma ferramenta que mantém um repositório de código aberto com suporte para controlo de versões. É uma ferramenta muito simples de usar e permite a colaboração de outras pessoas. A figura 2.2 mostra a ferramenta em acção para o projecto.

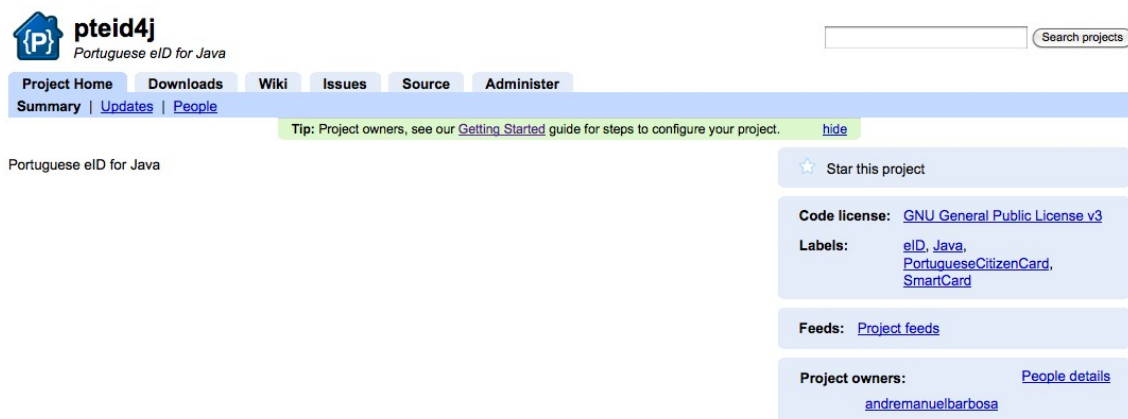


Figura 2.2: Google Code

2.3 Criptografia

A criptografia é o ramo da matemática responsável pelo estudo dos princípios e técnicas para encriptar e descriptar informação. O seu uso é especialmente visível no armazenamento

de informações sensíveis ou na transmissão de dados através de redes inseguras (como a Internet), de maneira a que o conteúdo das mensagens só possa ser lido pelo destinatário e não por qualquer outra pessoa que intercepte a comunicação.

Historicamente, a utilização da criptografia para transmissão de informação remonta ao tempo do Império Romano, onde o imperador Júlio César usava a forma mais básica de trocar as letras do conteúdo das mensagens que enviava para os seus generais por outras letras do alfabeto de maneira a que os mensageiros não conseguissem entender a mensagem [INCRYP]. Outro exemplo histórico da criptografia é o envio de mensagens encriptadas durante a 2ª Guerra Mundial pelo exército alemão, em que mais tarde os aliados viriam a decodificar o algoritmo de encriptação e, muitos historiadores afirmam, alterar o desenrolar da guerra [HSTCRYPT]. Muitas coisas podem ser ditas sobre a criptografia em si e sobre a sua importância na história, mas no âmbito da dissertação importa só perceber conceitos fundamentais e a forma como estes estão associados ao projecto.

2.3.1 Encriptação e Desencriptação

Em criptografia, a informação que pode ser lida e entendida sem qualquer tipo de medida especial ou transformação é conhecida como texto simples ou texto original. A encriptação é o processo de transformar esse texto através de um algoritmo, também conhecido como cifra, de maneira a que o texto resultante deste processo (texto encriptado) não possa ser lido e entendido por quem não possua o conhecimento de como a encriptação foi feita, ou seja, por quem não possua a chave da cifra. A desencriptação é simplesmente o processo inverso da encriptação, isto é, a obtenção do texto original com base no texto encriptado e na chave de encriptação. A figura 2.3 ilustra de forma simples os processos de encriptação e desencriptação [HSTCRYPT].

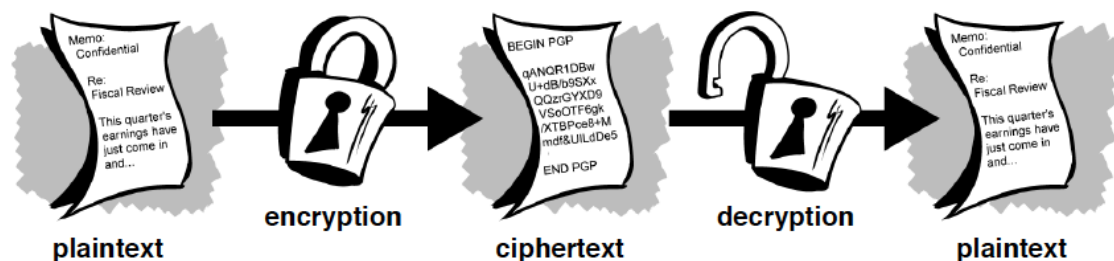


Figura 2.3: Encriptação e Desencriptação

2.3.1.1 Encriptação Simétrica

A encriptação simétrica, também conhecida como encriptação de chave secreta ou de chave simétrica, é a mais antiga e conhecida técnica da criptografia e caracteriza-se pelo uso de uma chave secreta, que pode ser um número, uma palavra ou apenas uma sequência de letras aleatórias [MS246071]. Esta chave é então aplicada ao texto da mensagem que se pretende que seja escondido através de um algoritmo de encriptação, e só o destinatário que possua a mesma chave consegue efectuar o processo inverso para obter o texto original da mensagem. O texto pode ser convertido simplesmente através da deslocação de caracteres de uma forma particular,

tal como o exemplo descrito acima do imperador Júlio César. A figura 2.4 ilustra o processo de encriptação simétrica HSTCRYPT.

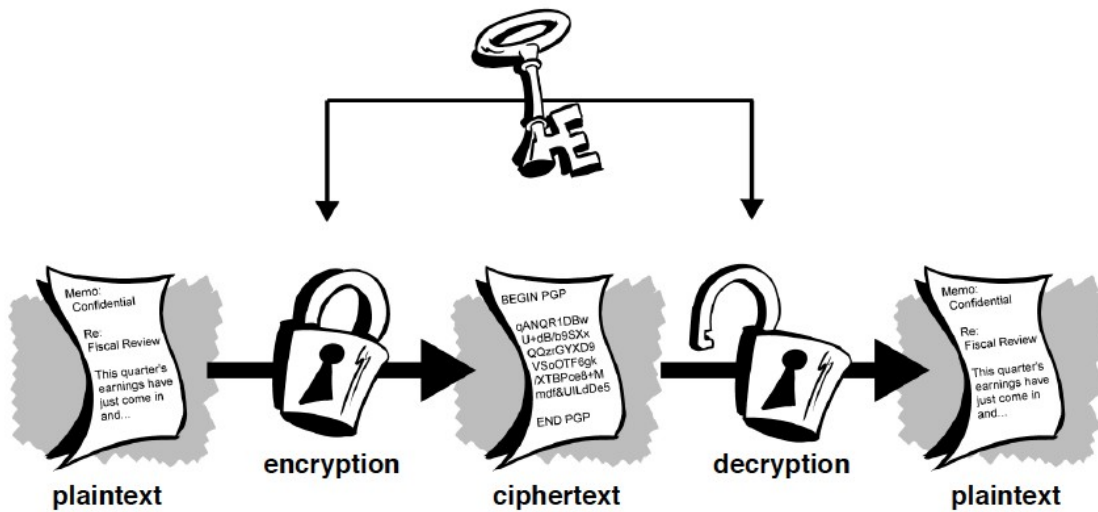


Figura 2.4: Encriptação Simétrica

Este tipo de encriptação tem a vantagem de ser computacionalmente muito rápida e é especialmente útil quando a informação encriptada não vai a lado nenhum, isto é, quando esta informação é sensível a alguns utilizadores e foi simplesmente encriptada para ser armazenada numa base de dados em que o administrador da mesma não deve poder ver o seu conteúdo, por exemplo. A grande desvantagem da criptografia convencional, como é também conhecida, é a distribuição da chave pelos destinatários, de maneira a que todos os intervenientes que podem visualizar o conteúdo de uma determinada mensagem o consigam fazer [INCRYP]. Dos algoritmos mais conhecidos que implementam este mecanismo fazem parte o DES, o Triple DES e o EAS, por exemplo.

2.3.1.2 Encriptação Assimétrica

Para colmatar a falha da troca das chaves secretas do método de encriptação anterior foi criada a encriptação assimétrica ou encriptação de chave pública, como é também conhecida. Esta técnica de encriptação é caracterizada por disponibilizar duas chaves para os processos de encriptação e desencriptação, uma privada e uma pública [MS246071]. A chave privada deve ficar apenas no remetente e nunca deve ser revelada a mais ninguém enquanto que a chave pública, como o nome indica, deve ser do conhecimento geral pelo menos para os utilizadores que possam vir a enviar mensagens encriptadas para esse destinatário. Se o processo de conversão de texto para conteúdo encriptado for efectuado com a chave privada, apenas quem possuir a chave pública pode efectuar a desencriptação novamente para o texto original, enquanto que se este processo for efectuado com a chave pública de um destinatário, apenas ele através da sua chave privada consegue replicar o conteúdo original de uma mensagem. A figura 2.5 ilustra o fluxo de eventos no processo de encriptação assimétrica [HSTCRYPT].

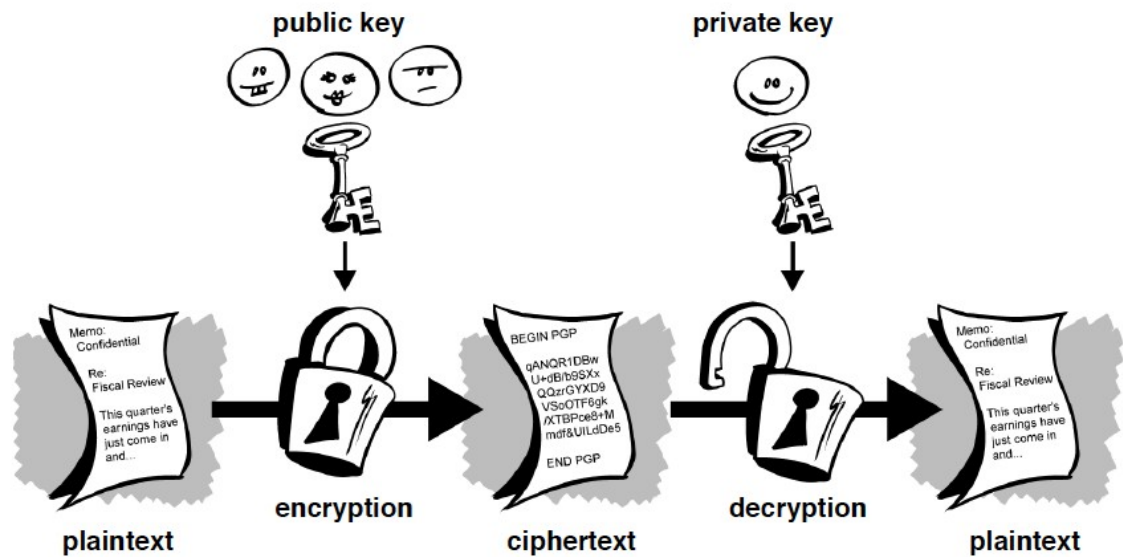


Figura 2.5: Encriptação Assimétrica

Comparativamente com a criptografia convencional, a encriptação assimétrica é bastante mais pesada computacionalmente, mas as suas vantagens na área de troca de informação sobre redes inseguras oferecem enormes benefícios aos utilizadores. Este tipo de criptografia não só remove a necessidade de transmissão da chave secreta ao destinatário de uma mensagem, como também permite que o remetente nem sequer precise de conhecer esse mesmo destinatário, para poder encriptar uma mensagem que lhe quer enviar ou desencriptar uma que outra pessoa lhe tenha enviado, desde que sejam utilizados de forma correcta as chaves públicas das entidades respectivas [INCRYP]. Algoritmos conhecidos que implementam este mecanismo passam pelo RSA, Diffie-Hellman e DAS, por exemplo, e dependendo do tamanho das chaves e o poder computacional existente oferecem vantagens distintas.

2.3.2 Assinaturas Digitais

A assinatura digital é um conjunto de instruções matemáticas baseadas na criptografia, que permite conferir autenticidade, privacidade e inviolabilidade sobre um determinado documento ou conjunto de dados. É uma das aplicações mais comum da encriptação assimétrica ou de chave pública, que permite ao destinatário de uma mensagem verificar a autenticidade da origem da informação e garantir que esta não foi alterada no caminho até ao destinatário. Objectivamente, a assinatura digital tem a mesma finalidade que a assinatura manuscrita mas oferece ainda outras vantagens como uma maior dificuldade de falsificação e o não-repúdio, isto é, o autor da mensagem não pode negar, ou não deve poder negar, que participou na sua elaboração [FCCN9929].

Os processos de assinatura digital num determinado documento ou conjunto de dados e a sua posterior verificação estão ilustrados na figura 2.6 e tal como podemos ver, o primeiro passo para a inserção de uma assinatura digital é a geração de uma sequência de caracteres (*hash* ou *message digest*) através de um algoritmo de dispersão [WIKIDSIG]. De seguida, essa cadeia de caracteres é encriptada através de um algoritmo de assinatura com a chave privada (certificado de assinatura) do autor da mensagem e o resultado desta encriptação é anexado ao texto original, dando origem ao que se chama de mensagem assinada digitalmente ou

electronicamente. A verificação da assinatura é feita através de dois processos em paralelo, onde o primeiro passa por gerar novamente uma sequência de caracteres com o mesmo algoritmo de dispersão a partir do texto original e o segundo diz respeito ao uso de um algoritmo de descriptação (inverso ao algoritmo de encriptação utilizado na inserção da assinatura), que, através da chave pública do remetente ou autor da mensagem, permite recriar a sequência de caracteres gerada pela função de dispersão no processo de assinatura. No final dos dois processos é feita uma comparação entre as duas cadeias de caracteres e em caso de sucesso a verificação é considerada válida, sendo que o oposto resulta na invalidação da assinatura.

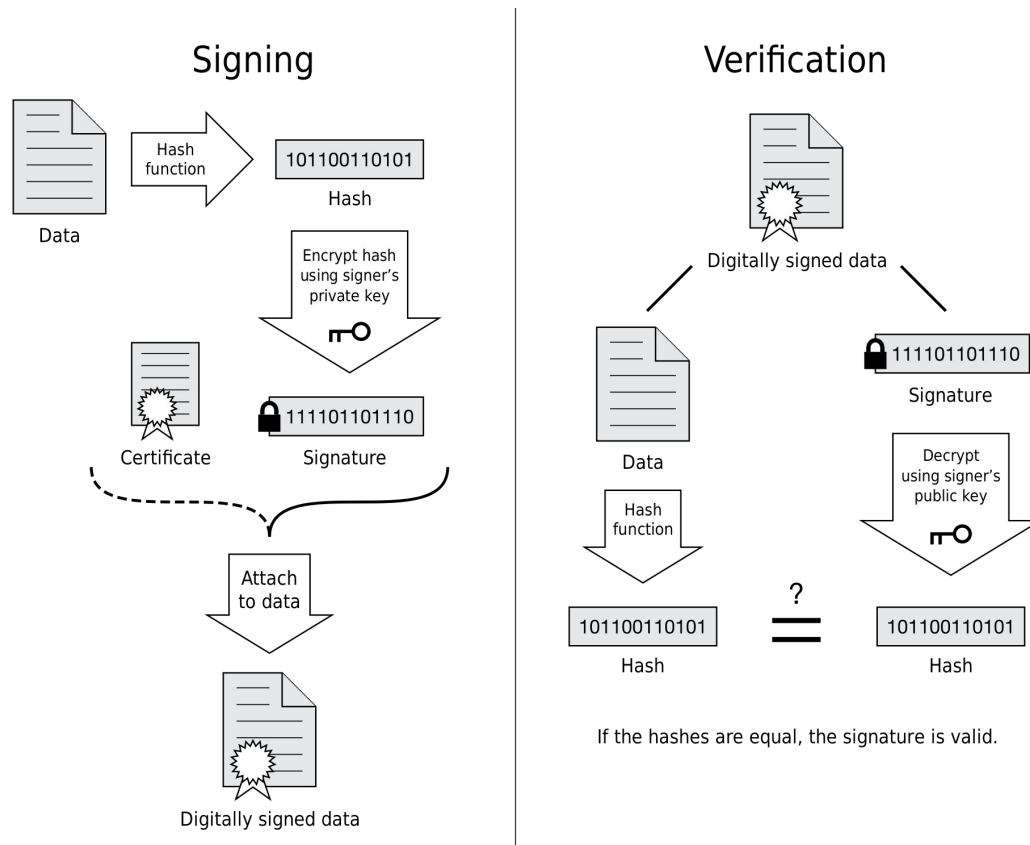


Figura 2.6: Diagrama dos processos de Assinatura Digital e Verificação da mesma

Para que uma assinatura digital seja considerada válida há que ter em conta também, além dos aspectos descritos acima, a validade do próprio certificado de assinatura. Mais detalhes sobre a validação de certificados digitais são apresentados na secção 2.3.3, mas por agora basta ter a noção da sua existência. É também importante mencionar que qualquer alteração no corpo da mensagem, por mínima que seja, depois de assinada invalida o processo de verificação da assinatura digital e consequentemente a assinatura em si.

2.3.2.1 Algoritmos de Dispersão

Os algoritmos ou funções de dispersão (*hash functions*) são procedimentos matemáticos que convertem um conjunto de dados com tamanho arbitrário numa sequência de caracteres com tamanho fixo pré-definido (*hash* ou *digest*). Estas funções devem ser executadas de forma relativamente rápida a nível computacional, de maneira a que possam ser utilizadas no mais comum dos computadores e devem também garantir que não existem conjuntos de dados

diferentes na entrada que dêem origem a dois blocos de caracteres iguais na saída. É também necessário garantir que não é possível, pelo menos sem um poder computacional quase infinito, reverter o processo de codificação e obter a mensagem original a partir da sequência de caracteres antes codificada num período de tempo relativamente curto. A figura 2.7 mostra um diagrama exemplo para a aplicação de algoritmos de dispersão sobre um conjunto de palavras.

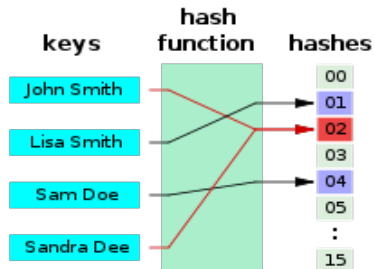


Figura 2.7: Diagrama Exemplo do uso de Algoritmos de Dispersão

Este tipo de funções criptográficas são aplicadas nas mais diversas áreas da informática com especial destaque para o armazenamento de palavras-passe numa base de dados para posterior validação unidireccional, por exemplo, e tal como foi mencionado acima na geração de blocos de caracteres codificados para a inserção de assinaturas digitais. MD5 e SHA-1 são dos algoritmos de dispersão mais usados nos dias de hoje, sendo que o último tem vindo a ganhar vantagem principalmente nas aplicações com assinaturas digitais. Ambos tiveram origem no MD4 e enquanto o MD5 gera um bloco com 128 bits o SHA-1 retorna um bloco ligeiramente maior com 160 bits. Está também disponível a família de algoritmos SHA-2, uma extensão à SHA-1, que oferece um aumento da resistência a ataques consideráveis.

2.3.2.2 Selos Temporais

O selo temporal, ou em inglês *Timestamp*, é uma sequência de caracteres numa estrutura pré-definida, que representa a hora e data actual de um determinado sistema. A sua utilização é especialmente importante nas assinaturas digitais porque permite, além da garantia do não-repúdio e da integridade da origem, esta extensão garante ao documento assinado também uma validação da data de inserção da assinatura, neste caso concreto.

Para que um selo temporal seja considerado fidedigno é preciso que este seja assinado por uma autoridade de certificação de selos temporais (TSA, do inglês *Time Stamping Authority*). O processo de inserção de um selo temporal válido, conhecido como *trusted time-stamping*, está ilustrado na figura 2.8 [WIKITSTP]. É executada uma função de dispersão (*hash*) sobre os dados para os quais se quer obter o selo temporal de confiança, e o bloco resultante é enviado para a TSA, que depois de o concatenar um selo temporal, executa uma função de dispersão sobre este novo conjunto (bloco + selo temporal). Para que o novo bloco seja considerado então de confiança a TSA deve aplicar a sua chave privada sobre o conjunto anterior, concatenar novamente com o selo temporal e enviar o resultado final de volta para a entidade que está a pedir o serviço. Este bloco do selo temporal assinado mais o próprio selo temporal em formato extenso, devem ser anexados aos dados originais.

Trusted timestamping

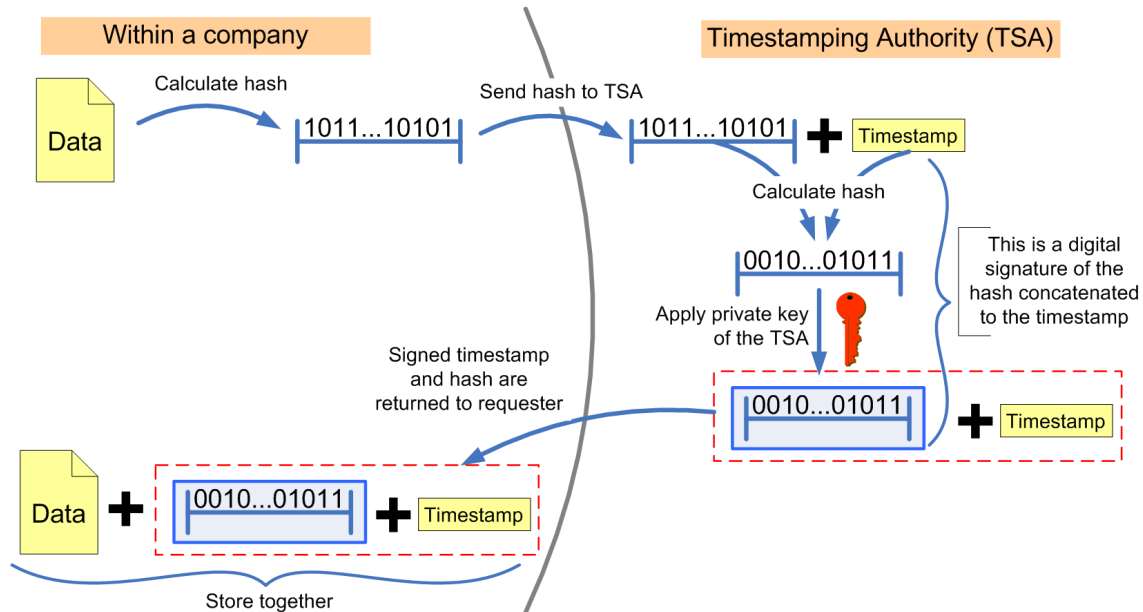


Figura 2.8: Diagrama de Inserção de um Selo Temporal num Documento

2.3.2.3 Legislação

O documento electrónico susceptível de representação como declaração escrita, ao qual tenha sido aposta uma Assinatura Electrónica Qualificada, faz prova plena das declarações atribuídas ao seu autor, sem prejuízo da arguição e prova da falsidade do documento.

O valor probatório de documento electrónico a que não tenha sido aposta uma Assinatura Electrónica apreciado nos termos gerais de direito, salvo existência de válida convenção em sentido diverso.

2.3.3 Certificados Digitais

Os certificados digitais são documentos electrónicos únicos, assinados digitalmente que contém um conjunto de informações sobre as entidades (pessoas ou instituições) para as quais foram emitidos. Este tipo de ficheiros são emitidos por uma Autoridade de Certificação (AC) e o seu principal objectivo é garantir que a chave pública contida no certificado pertence à entidade para a qual o certificado foi emitido [MS195724]. A figura 2.9 ilustra o conceito de certificado digital tal como foi descrito neste parágrafo.

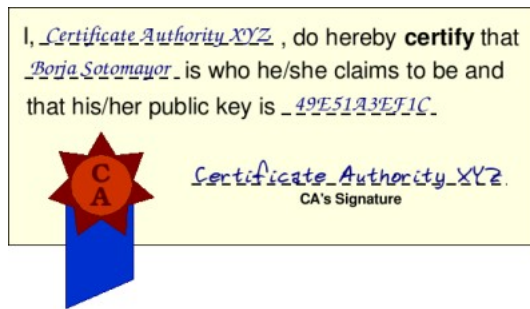


Figura 2.9: Ilustração da finalidade de um Certificado Digital

Imaginemos o cenário em que, num determinado ambiente público, a entidade A pretende enviar dados encriptados para a entidade B de forma a que só esta última consiga descriptar o conteúdo da mensagem. Para o fazer, a entidade A deve obter a chave pública da entidade B de maneira a conseguir fazer a encriptação da informação pretendida. Até aqui tudo bem, excepto que se existir uma entidade C que, através de um ataque do homem no meio (*man-in-the-middle attack*), consiga iludir a entidade A e lhe envie uma falsa chave pública da entidade B, fazendo com que a entidade C tenha a chave privada capaz de descriptar o conteúdo da mensagem destinada à entidade B [CISSP08]. É aqui que entram os certificados digitais de maneira a garantir que, se a AC emissora do certificado digital da chave pública da entidade B for da confiança da entidade A, então esta pode confiar na origem da chave. A figura 2.10 mostra uma diagrama ilustrativo de um ataque do homem no meio.

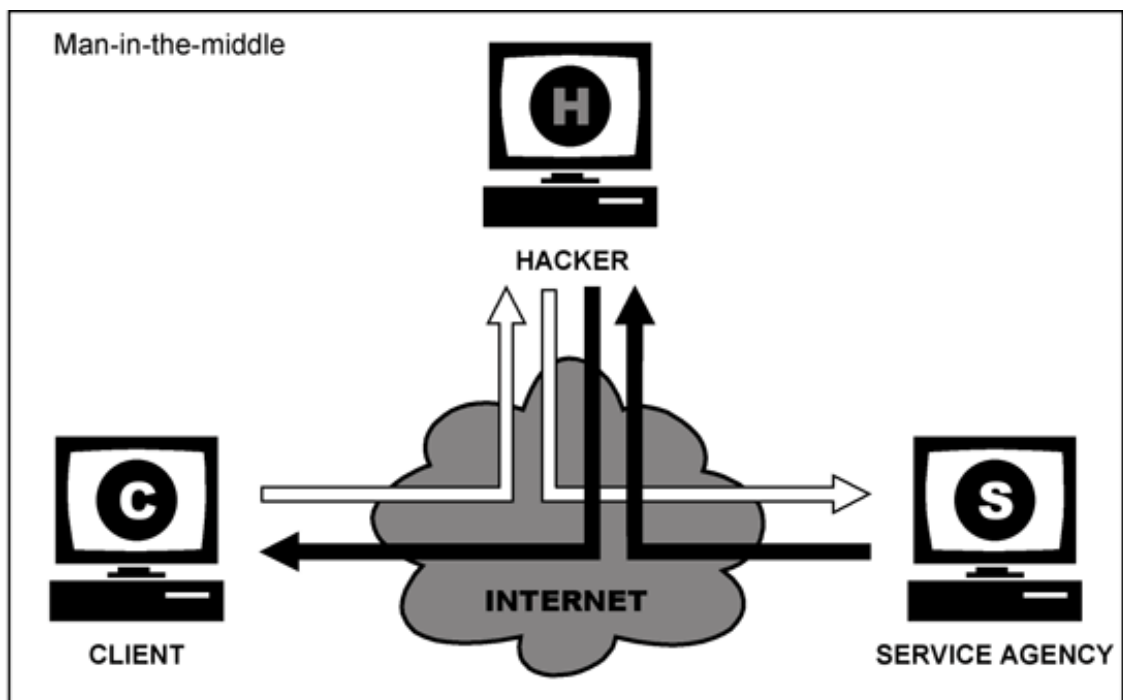


Figura 2.10: Ataque do Homem no Meio

Da composição dos certificados digitais fazem parte uma chave pública, informação sobre o certificado (dados sobre a identidade da entidade como nome, código de utilizador, morada

e/ou outros) e uma ou mais assinaturas digitais. Resumidamente, um certificado digital é uma chave pública com uma ou duas formas de identificação mais um carimbo de certificação de uma entidade de confiança. A partilha dos certificados num ambiente público de uma forma estruturada é gerida através de uma Infra-estrutura de Chaves Públicas (ICP).

2.3.3.1 Autoridades de Certificação

Uma Autoridade de Certificação (AC), ou em inglês *Certificate Authority (CA)*, é uma entidade terceira e independente reconhecida como fidedigna que é responsável por emitir e assinar certificados digitais. Se uma determinada entidade confia numa AC, então tem de assumir como válida toda a informação contida num certificado que tenha sido emitido pela mesma, desde a chave pública, passando pela data de validade desse certificado, até ao nome da entidade associada ao certificado, entre outros dados.

Como parte de uma PKI, é da responsabilidade da AC verificar junto de uma Autoridade de Registo (AR), ou em inglês *Registration Authority (RA)*, a identidade da entidade que está a solicitar a emissão de um certificado, bem como todas as informações nele contido, antes de proceder à emissão do mesmo. Se a AR validar com sucesso os dados dessa entidade, então o certificado pode ser emitido pela AC.

2.3.3.2 Infra-estruturas de Chaves Públicas

Uma Infra-estrutura de Chaves Públicas (ICP), ou em inglês *Public Key Infrastructure (PKI)*, é o conjunto de dispositivos, aplicações, pessoas, políticas e procedimentos necessários para a criação, gestão, distribuição, uso, armazenamento e revogação de certificados digitais. Só com uma combinação bem definida de protocolos, tecnologias, infra-estruturas, serviços e políticas de emissão de certificados, é que uma organização pode funcionar como uma PKI. O diagrama da figura 2.11 mostra a troca de informação dentro daquilo que é uma infra-estrutura deste género.

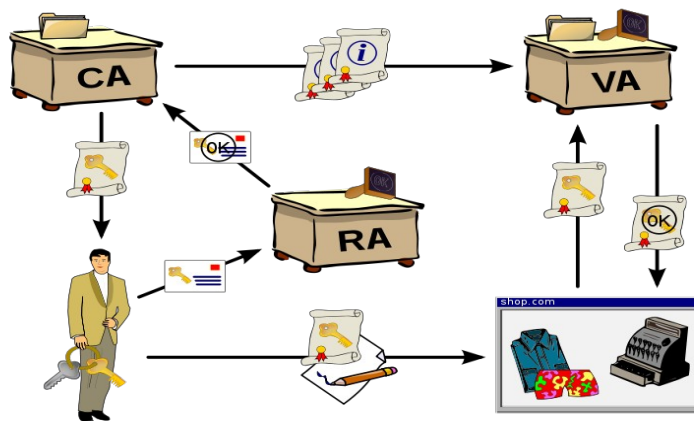


Figura 2.11: Diagrama de uma Infra-estrutura de Chaves Públicas

Tal como se pode ver no diagrama acima, e como tinha sido descrito na secção anterior, as autoridades de certificação (AC), desempenham um papel muito importante dentro de uma PKI, pelo que são estas as responsáveis pela emissão dos certificados digitais para as entidades em questão. O papel de uma AC passa então pela assinatura (certificação) da chave pública da

entidade que, consoante as aplicações, será enviada ou consultada por outros elementos dentro da PKI, que terão de efectuar a sua validade dentro da infra-estrutura em questão.

2.3.3.3 Listas de Revogação de Certificados

As Listas de Revogação de Certificados (LRC), ou em inglês *Certificate Revocation Lists* (CRL), são listas de certificados que foram revogados ou que deixaram de ser válidos, logo não são de confiança. Este tipo de listas estão normalmente presentes em qualquer PKI como forma de manter toda a estrutura de chaves públicas consistente e segura.

Como alternativa à utilização de CRL, existe também o *Online Certificate Status Protocol* (OCSP) que, em alguns casos, veio substituir o primeiro método de validação de certificados X.509. O protocolo OCSP utiliza uma estrutura pedido/resposta via Internet aos servidores que suportam uma determinada PKI, onde envia e identificador do certificado sobre o qual pretende saber o estado de validade, e como resposta recebe uma mensagem desse servidor, devidamente assinada, a atentar ou não a validade do certificado em questão.

2.4 Cartão de Cidadão

O Cartão de Cidadão (CC) é o novo documento de cidadania dos portugueses, sem limite mínimo de idade, e começou a ser emitido entre 2006 e 2007 durante um período experimental nos Açores, sendo que até ao presente momento foram emitidos mais de 2,5 milhões de cartões, dos quais 44% têm assinatura electrónica qualificada activa [CCSTS10]. O novo documento substitui o bilhete de identidade, o cartão de beneficiário da Segurança Social, o cartão de utente do Serviço Nacional de Saúde, o cartão de contribuinte e o cartão de eleitor e distingui-se dos restantes pelas capacidades electrónicas associadas, não só permite a identificação presencial tal como os outros documentos mas introduz um novo tipo de identificação dos cidadãos de uma forma electrónica segura.



Figura 2.12: Logotipo do Cartão de Cidadão

Neste projecto dinamizador da modernização da Administração pública de Portugal, amigo do desenvolvimento tecnológico e enquadrado no plano de inovação do Governo, estiveram envolvidas várias entidades de renome nacional e internacional, das quais podemos destacar por exemplo Microsoft, Siemens, Accenture, Multicert e Critical [CCPVC08]. Interessa perceber, do ponto de vista da dissertação, quais as potencialidades e limitações do CC não só no que diz respeito ao campo tecnológico, mas também à legislação associada ao cartão e consequentes restrições impostas a nível de protecção de dados e estatutos legais.

2.4.1 Objectivos

A Agência para a Modernização Administrativa (AMA), entidade do Governo responsável pela gestão do projecto Cartão de Cidadão, identifica para o CC objectivos em quatro áreas

distintas: como documento de identificação, como projecto de modernização, como projecto tecnológico e como garantia dos direitos do cidadão no mundo digital [CCOBV08].

Como documento de identificação, o CC deve permitir ao cidadão a sua identificação visual e presencial quando requerida pelas autoridades competentes e a sua identificação electrónica nos actos informatizados que intervenha. Além da substituição dos documentos mencionados acima, o CC deve também permitir a interacção com diferentes entidades públicas e privadas e assegurar mecanismos de segurança que dificultem a falsificação da identidade do cidadão e invasão da privacidade do mesmo, de maneira a que os dados do cartão só sejam acedidos com o consentimento prévio do seu portador.

Como projecto de modernização integrado na política de modernização da Administração pública do país, e tendo em conta as questões associadas a esta metodologia como simplificação, agregação, segurança e desmaterialização, o CC deve garantir ao cidadão uma maior segurança na identificação e uma uniformização no sistema de identificação civil de acordo com as normas da União Europeia (UE). O cartão deve também facilitar a vida do cidadão pela necessidade física de menos cartões e pela melhoria da relação entre este e os serviços públicos a nível de qualidade e rapidez de execução dos processos. Do ponto de vista tecnológico, o CC deve ainda promover a sua utilização nos serviços electrónicos, desde mecanismos de autenticação até assinatura digital de documentos, e estimular um aumento da competitividade nacional com novas abordagens à maneira como os serviços públicos são prestados pelo Estado.

Como projecto tecnológico, o CC deve melhorar o acesso aos serviços públicos com a redução de barreiras e a diversificação dos meios de acesso e simplificar os processos ligados à administração com a adaptação às novas tecnologias. Os serviços públicos devem também ser integrados a nível de partilha de dados e a nível da interoperabilidade entre aplicações das várias entidades administrativas e a gestão das bases de dados associadas ao CC, ou a qualquer outro serviço relacionado com o cidadão, deve ser feita com extrema segurança e responsabilidade, sem nunca por em causa os direitos do cidadão.

Como garantia dos direitos do cidadão num mundo digital, no que diz respeito à recolha e tratamento de dados do cidadão e à informação que é transmitida nas ligações aos diferentes serviços, o CC não poderá conter dados sobre a situação fiscal, de saúde ou de segurança social do seu titular, sendo que esta informação está armazenada em cada um dos organismos a que diz respeito. Do ponto de vista electrónico, não deverá ser possível reconstituir a informação relativa à vida do cidadão e, mais uma vez, qualquer acesso digital aos dados pessoais do cidadão só pode ser feito com o consentimento prévio do mesmo.

2.4.2 Características

As características do Cartão de Cidadão estão divididas em três áreas distintas: físico, visual e electrónico. Do aspecto físico do CC sabemos que tem um formato Smart Card e substitui o bilhete de identidade, o cartão de contribuinte, o cartão de beneficiário da Segurança Social, o cartão de eleitor e o cartão de utente do Serviço Nacional de Saúde [CCCRCT]. Do ponto de vista visual, a figura 2.13 ilustra o tipo de informação que é apresentado no CC. Mais características físicas e técnicas do cartão podem ser encontradas no Anexo A: Especificações Técnicas do Cartão de Cidadão.

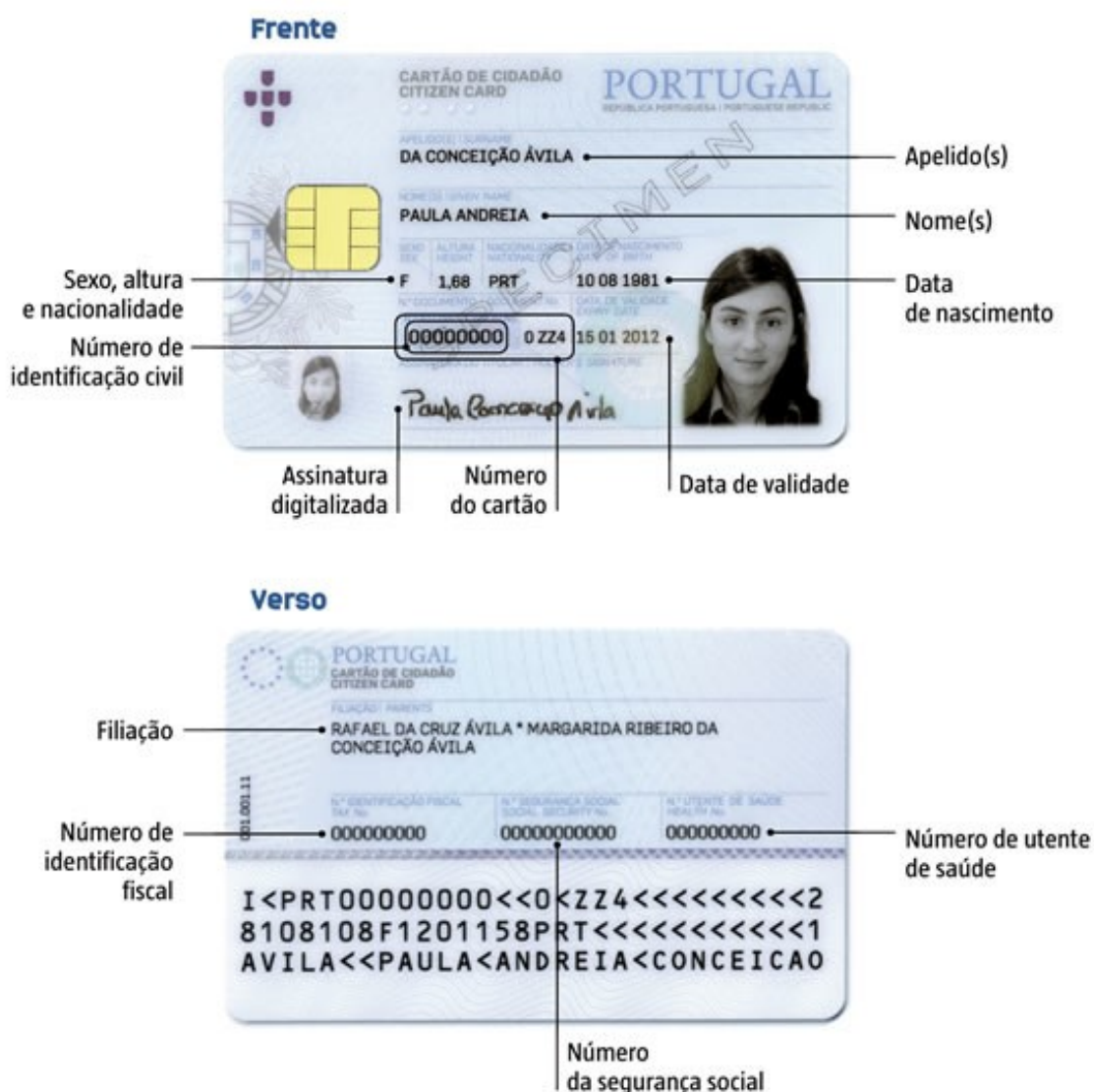


Figura 2.13: Aspecto Físico do Cartão de Cidadão

Por último, e mais importante no contexto da dissertação, do ponto de vista electrónico o CC possui um chip de contacto com dois certificados digitais, um para autenticação e outro para assinaturas digitais, e a informação visual do cartão está também contida no interior do chip, juntamente com a morada do cidadão em causa.

2.4.3 Entidades de Certificação

No âmbito do Cartão de Cidadão, foram criados diversos organismos responsáveis pela emissão e gestão dos certificados digitais presentes nos cartões. Estas entidades estão debaixo da alçada do Estado e para que esses certificados sejam considerados válidos numa máquina é necessário que essa cadeia de certificados seja devidamente instalada. Para isso, é importante conhecer primeiro essa estrutura, de maneira a saber os passos necessários para a instalação.

2.4.3.1 SCEE

O Sistema de Certificação Electrónica do Estado (SCEE) é uma entidade do Estado que visa assegurar a unidade, a integração e a eficácia dos sistemas de autenticação na relação entre as pessoas colectivas e singulares com o Estado e entre entidades públicas. É a entidade gestora do certificado raiz do Estado, que está no topo da hierarquia de todos os outros certificados associados ao Estado, incluindo o da EC do Cartão de Cidadão.

2.4.3.2 Hierarquia

A cadeia de certificados necessária para a validação completa dos certificados presentes no Cartão de Cidadão envolve, além do certificado raiz do Estado emitido pela SCEE, as seguintes Entidades de Certificação:

- EC do Cidadão: assina as sub-ECs na hierarquia PKI do CC e emite alguns certificados digitais para serviços do CC (timestamp, OCSP, servidores web, ...);
- Sub-EC de Autenticação do Cidadão: responsável pela emissão de certificados digitais de autenticação em formato X509v3, presente em cada Cartão de Cidadão;
- Sub-EC de Assinatura do Cidadão: responsável pela emissão de certificados digitais de assinatura qualificada em formato X509v3, presente em cada Cartão de Cidadão;
- Sub-EC de Controlo de Acessos: Responsável pela emissão de certificados digitais de Organismos, em formato CVC.

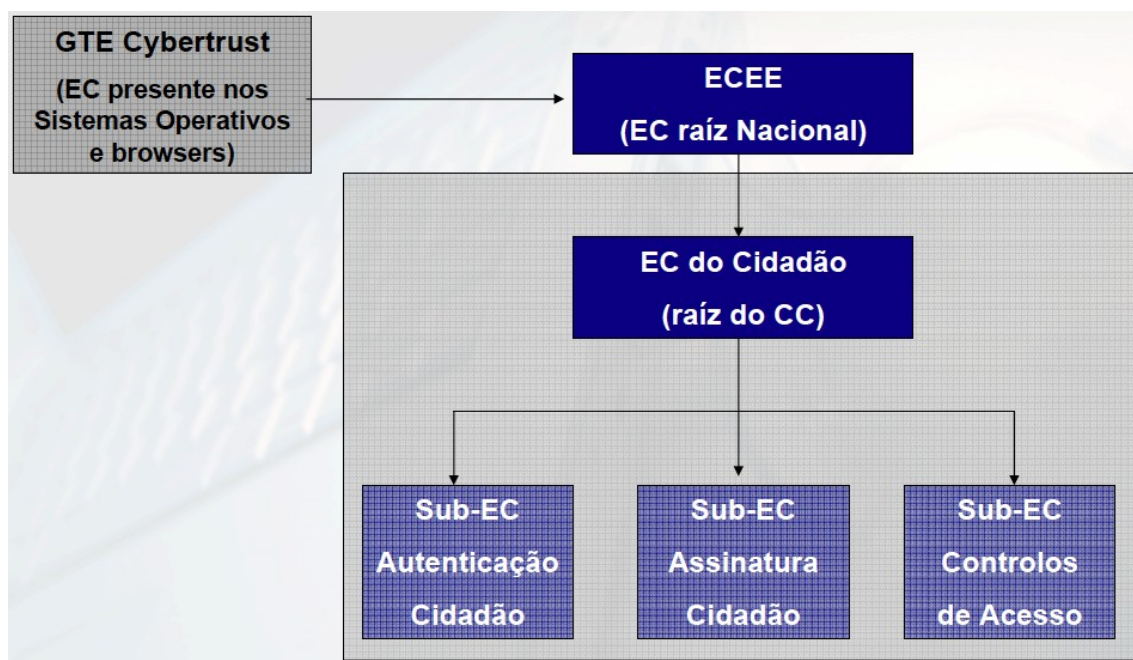


Figura 2.14: Hierarquia das Entidades de Certificação do Cartão de Cidadão

A figura 2.14 apresenta graficamente a hierarquia descrita nesta secção e a maneira como as diferentes Entidades de Certificação se relacionam.

2.4.4 Casos de Estudo

Muitas são as entidades que começam a procurar as mais diversas soluções de integração com o Cartão de Cidadão, tendo algumas conseguido esse objectivo com sucesso. Apesar desse sucesso na utilização do cartão como mecanismo de autenticação em algumas páginas web, não foi conseguimos descobrir nenhuma solução que implementasse a funcionalidade da assinatura digital na web. E se é verdade que algumas das empresas a desenvolver camadas de código sobre o CC afirmam que o fazem, não existe nenhuma demonstração disponível para consulta.

Optámos por deixar de fora desta listagem os casos dos portais públicos, como o Portal do Cidadão e o Portal da Empresa, porque a relação entre o cidadão e o Estado é o objectivo básico da introdução do CC na sociedade portuguesa. Interessante é perceber até que ponto a relação dos cidadãos com as entidades privadas melhora, com a introdução destes novos mecanismos e o que de inovador se pode apresentar nesse campo.

2.4.4.1 SAPO

Pioneiro em Portugal em muitos aspectos, o SAPO foi das primeiras entidades privadas a colocar no seu portal a autenticação com o Cartão de Cidadão dos seus utilizadores. A figura 2.15 mostra o formulário disponível actualmente no portal do SAPO, onde se pode visualizar, juntamente com a autenticação básica e o OpenID, a autenticação por CC.



The image shows a web interface for logging in to SAPO. At the top, there is a header with a green frog icon and the word 'login' in large black letters. Below this, there are three buttons: 'sapo', 'OpenID', and 'CARTÃO DE CIDADÃO'. The 'CARTÃO DE CIDADÃO' button is highlighted. Below the buttons, there is a section titled 'Entre com o seu Cartão de Cidadão'. Inside this section, there is a yellow box with a blue 'C' icon and the text: 'Para fazer login com o **Cartão de Cidadão Português** deve ligar o **leitor de cartões** e assegurar-se que o software está correctamente instalado.' Below this box, there are three numbered steps: 1. Insira o cartão no seu leitor. 2. Clique no botão para **validar**. 3. Introduza o PIN do cartão. At the bottom of the section, there is a green button labeled 'Validar' and a link labeled 'Ajuda'.

Figura 2.15: Autenticação no SAPO com Cartão de Cidadão

2.4.4.2 IST

Um caso de estudo ainda mais interessante do ponto de vista da dissertação, por se tratar de um ambiente académico, é o caso do Instituto Superior Técnico (IST), que disponibiliza aos seus utilizadores actualmente o mecanismo de autenticação com o Cartão de Cidadão. Ao contrário da SAPO, juntamente com a autenticação básica e a autenticação por CC, o IST disponibiliza a autenticação por Kerberos, tal como o formulário da figura 2.17 ilustra.



Figura 2.16: Autenticação no IST com o Cartão de Cidadão

2.5 Java

Do ponto de vista de integração com a base de dados do sistema actual, é de esperar que qualquer implementação que não possa ser realizada em PL/SQL, seja transportada para a Java Virtual Machine (JVM) da Oracle. Resumindo, qualquer mecanismo que recorra à utilização de código Java para o seu funcionamento pode ser facilmente inserido na base de dados.



Figura 2.17:
Logotipo do Java

2.5.1 iText

O iText é uma biblioteca Java com distribuição livre, desenvolvida em código aberto, para a criação e manipulação de ficheiros PDF. De todas as funcionalidades que a biblioteca dispõe é especialmente importante a opção de inserção de assinaturas digitais a partir de um certificado digital. Está também disponível uma API bastante completa para a sua utilização.



Figura 2.18:
Logotipo do iText

2.5.2 eID Applet

O projecto eID Applet é um componente para os navegadores para a utilização do cartão de identificação belga na web. Esta aplicação incorpora todos os mecanismos para acesso ao Smart Card através de uma applet Java. Sendo o Cartão de Cidadão português bastante semelhante belga em muitos aspectos é importante perceber a estrutura desta biblioteca de maneira a que uma implementação, também ela semelhante, possa ser efectuada para o CC. Também este projecto foi desenvolvido em código aberto e está à disposição gratuitamente. Sem querer entrar numa discussão sobre atitudes e personalidades, é neste tipo de pormenores que por vezes se nota a diferença entre Portugal e o resto da Europa. Enquanto que, só na Bélgica, foi possível uma série de possíveis implementações para o acesso ao cartão de identificação, com as mais diversas funcionalidades, e quase todas em código aberto multi-plataforma, aqui em Portugal o pouco que pode encontrar ou é comercial ou só é aplicável a uma tecnologia específica. Não obstante, o eID Applet parece ser a solução livre mais completa disponível no mercado.

2.6 Oracle

É importante percebermos dentro de uma base de dados Oracle, quais são as opções que temos relativamente aos mecanismos que pretendemos implementar no decorrer da dissertação. Com esse objectivo em mente, foram analisados as ofertas dentro da Oracle que pudessem de alguma forma satisfazer estas necessidades. Essa pesquisa culmina num módulo disponibilizado pela empresa para versões da base de dados 10gR2 ou superior a que deram o nome de Segurança Avançada da Oracle (OAS, em inglês). Nesta secção é apresentada uma análise dessa tecnologia, das vantagens e desvantagens.



Figura 2.19: Logotipo da Oracle

2.6.1 Segurança Avançada

O módulo OAS é uma opção de segurança para as base de dados Oracle que incorpora três serviços distintos: encriptação transparente de dados, encriptação na rede e autenticação forte. Destes, o que mais nos interessa é o primeiro, para a componente de encriptação de conteúdos da base dados, que possa ser integrado de alguma forma com o Cartão de Cidadão. Um pormenor que chama imediatamente a atenção neste pacote da Oracle é o custo da licença, com um valor de 11,000\$ por processador. Se tivermos em conta que só a FEUP tem no seu servidor 8 processadores para suporta a base de dados, isso significaria um custo na ordem dos 88,000\$.



Figura 2.20: Diagrama de Funcionamento da Segurança Avançada da Oracle

2.6.1.1 Encriptação Transparente de Dados

A Encriptação Transparente de Dados (TDE, em inglês), é uma tecnologia disponibilizada pela Oracle para a sua base de dados num módulo de segurança avançada. No meu modo de

funcionamento não necessita de fazer nenhuma alteração estrutural nas bases de dados dos sistemas existentes, isto é, não é necessária a inclusão de vistas por cima das tabelas que se quer esconder ou TRIGGERS de selecção. Para que uma coluna de uma tabela seja automaticamente encriptada, basta mudar o tipo de dados para ENCRYPT e o sistema faz o resto. As chaves de encriptação são armazenadas num sistema central (Oracle Wallet) que, consoante uma validação prévia, as disponibiliza ou não para o mecanismo de desencriptação. O diagrama da figura 2.21 suporta aquilo que foi apresentado neste parágrafo sobre a tecnologia TDE da Oracle.

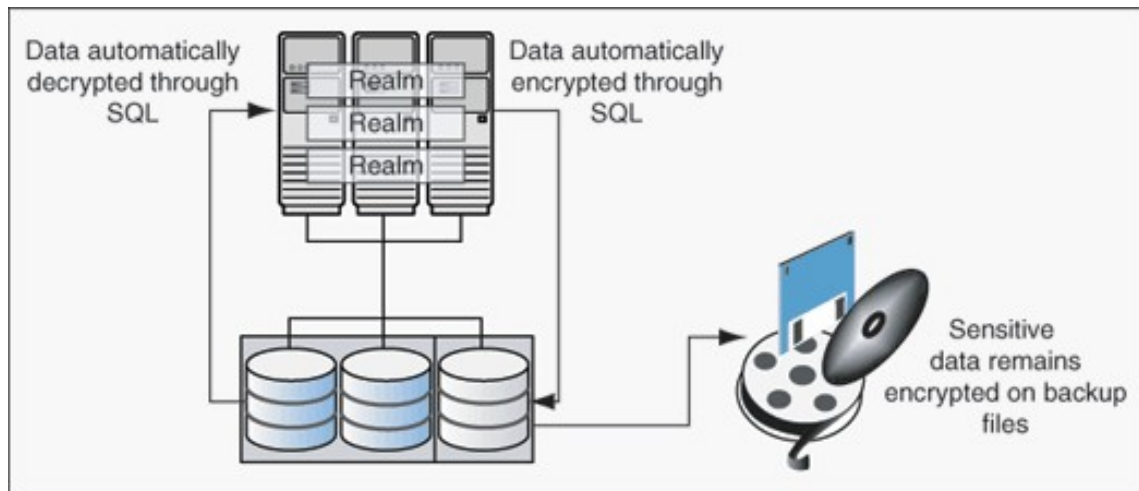


Figura 2.21: Diagrama da Encriptação Transparente de Dados da Oracle

Depois de entendermos bem o que a componente TDE da Oracle representa como solução para armazenamento de dados encriptados, é insensato pensar que é possível implementar uma solução semelhante através de código externo, isto é, tendo em conta que esta componente da base de dados actua num nível baixo da estrutura da Oracle, não é possível desenvolver código que tenha acesso a essa camada da estrutura da base de dados. Assim, qualquer solução para a encriptação de dados que não esta terá de ser necessariamente mais complexa e irá representar um esforço mais ou menos grande de alterações necessárias.

2.7 Resumo

Ao longo deste capítulo foram apresentados diversos conceitos que estão associados à dissertação, directa ou indirectamente. Todos estes conceitos fazem parte da revisão tecnológica do projecto e de serão utilizados de alguma forma na implementação, quer através da sua inclusão imediata, quer em componentes que implementam soluções semelhantes. Os conceitos teóricos ajudam a perceber o modelo necessário de suporte à estrutura a implementar e às limitações ou restrições importas pelo uso das respectivas metodologias.

3 Descrição do Problema

Neste capítulo é feita uma descrição mais detalhada do problema em concreto, com o uso do Cartão de Cidadão como mecanismo de autenticação em sistemas de informação num ambiente académico. São descritos todos os cenários de utilização nas diversas vertentes como autenticação, assinatura digital e encriptação, assim como as vantagens, desvantagens e lugar na lista de prioridades de implementação do projecto. No decorrer deste capítulo são identificados os objectivos específicos que se pretende atingir em cada caso concreto assim como as possíveis barreiras que irão ser encontradas pelo caminho até à sua implementação.

3.1 Introdução

Tendo em conta o universo da UP actualmente com cerca de 29.000 estudantes, 2.300 professores e investigadores e 1.700 funcionários não docentes [UPAP09], qualquer mudança estrutural de fundo na maneira como as coisas funcionam na organização e, no caso concreto, no seu SI, tem de ser muito bem pensada e organizada para evitar constrangimentos graves nos 33.000 membros da instituição. Ao longo deste capítulo vão ser descritos os cenários de utilização do CC como mecanismo de autenticação, as suas vantagens e desvantagens, e o impacto que as alterações provocadas por estes procedimentos de segurança de informação pode causar na vida dos alunos e funcionários da UP.

Num momento em que a sociedade portuguesa atravessa uma crise profunda de confiança no sistema, nas entidades públicas e no Estado em geral aliada à situação económica instável do país, é importante que o Cartão de Cidadão consiga estabelecer uma pequena relação de mútua confiança com os cidadãos portugueses. Para que isso aconteça, e no nosso caso em concreto, temos de definir procedimentos de segurança com riscos mínimos ou quase nulos para que uma instituição pública como a UP mantenha a credibilidade que merece junto dos seus utilizadores e lhes transmita uma sensação de confiança.

3.2 Cenários de Utilização

As funcionalidades disponibilizadas pelo Cartão de Cidadão abrem portas a uma série de potencialidades, que podem ser usadas tanto no sector público como no sector privado. No

âmbito desta dissertação e tendo em conta aquilo que é o mundo académico de que a FEUP faz parte e das aplicações que a Sysnovare pretende desenvolver é necessária a criação de algumas barreiras, metas que podem ser atingidas durante o decorrer do projecto e outras que deixem a corrida em aberto para um futuro próximo onde a uniformização da utilização do Cartão de Cidadão seja uma realidade na sociedade portuguesa.

3.2.1 Autenticação

Apesar das mudanças introduzidas a nível electrónico, o cartão continua a servir como principal meio de identificação perante as entidades públicas como a polícia, finanças, hospitais e centros de saúde. No fundo, no que diz respeito à identificação em pessoa o Cartão de Cidadão, tem o mesmo valor legal que o bilhete de identidade ou o cartão de contribuinte perante as entidades interessadas. A inovação prende-se com as potencialidades digitais associadas à autenticação do cidadão e sobre estas pretende-se analisar os cenários descritos a seguir.

3.2.1.1 Autenticação de Utilizadores

Num mundo com milhões de aplicações web e com milhares a serem criadas todos os dias, é cada vez mais difícil gerir as diversas contas que temos espalhadas na Internet. Os muitos códigos de utilizadores e senhas de acesso para dezenas ou centenas de páginas diferentes podem ser um verdadeiro pesadelo de manter. Aliado a um fenómeno de insegurança e desconfiança cada vez mais acentuado sobre os sistemas informáticos que se tem espalhado recentemente um pouco por todo o mundo, a autenticação através do Cartão de Cidadão, é sem dúvida um passo certo no caminho para re-estabelecer a confiança dos utilizadores nas aplicações, principalmente nas que contém informações mais sensíveis. É, por isso, importante para a UP, ser pioneira neste tipo de autenticação e apresentar mecanismos que transmitam aos seus utilizadores a confiança que estes esperam de sistemas informáticos desenvolvidos pela Instituição que os acolhe e prepara para o futuro.

3.2.1.1.1 Descrição

Para que um utilizador da instituição se possa autenticar com o Cartão de Cidadão, deverá associar o documento à sua conta de utilizador do SI, por exemplo através da sua área de administração pessoal ou através de uma ligação dentro da página de autenticação. Esta associação será feita através do número de documento do Cartão de Cidadão, que pode ser inserido previamente por alguém dos serviços administrativos da instituição e validado contra o cartão presente no leitor no momento de associação, ou pode ser retirado nesse instante do cartão e associado à conta do utilizador.

3.2.1.1.2 Actores

- Utilizadores da instituição;

3.2.1.1.3 Vantagens

- Uniformização da autenticação em aplicações distintas, desde instituições públicas a empresas privadas;

Descrição do Problema

- Maior garantia de que o utilizador é efectivamente quem se autenticou visto que é necessária a presença física do cartão e a introdução do PIN de acesso para efectuar a autenticação no SI.

3.2.1.1.4 Desvantagens

- Perda ou roubo do cartão pelo utilizador pode levantar algumas questões de segurança ou de logística visto que enquanto o cidadão não estiver na presença da 2ª via do cartão terá de voltar a usar o método de autenticação antigo ou não poderá aceder à aplicação;
- Necessidade de aquisição de leitores de cartões Smart Card a disponibilizar pelas instalações da instituição, o que pode dar origem a alguma reprovação por parte do departamento financeiro.

3.2.1.1.5 Viabilidade de Implementação

A implementação dos mecanismos de autenticação com o Cartão de Cidadão no SI é sem dúvida uma das prioridades na dissertação, tanto no âmbito da FEUP como da Sysnovare, e é de esperar que esta funcionalidade seja implementada antes do final do projecto.

3.2.1.2 Identificação de Pessoas Externas

Numa instituição de ensino superior, como em muitas outras instituições públicas ou privadas, a interacção com entidades externas é não só uma mais-valia por partilha de recursos e conhecimento, como por vezes uma necessidade sem a qual muitas instituições não conseguiriam sobreviver no mundo actual. Um lado negativo desta situação é que muitas vezes, não se conhecem previamente as pessoas com as quais uma instituição tem de interagir e por vezes dar acesso aos seus recursos, o que levanta à partida uma enorme sensação de insegurança.

A nível presencial, a apresentação de um documento de identificação com fotografia, como o bilhete de identidade ou carta de condução, resolve facilmente esta barreira mas, num universo cada vez mais digital onde as pessoas se cruzam menos fisicamente, é extremamente importante criar mecanismos de identificação que transmitam aos responsáveis de uma instituição uma elevada sensação de confiança e segurança quando estes dão acesso a informações mais ou menos sensíveis a pessoas que na maior parte dos casos nunca viram na vida.

3.2.1.2.1 Descrição

Este cenário tem dois casos: o registo inicial de um utilizador já conhecido, como sucede, por exemplo, com os novos estudantes admitidos pelo concurso nacional; e o registo de um utilizador completamente desconhecido. Relativamente ao primeiro caso, o sistema deverá saber, previamente, qual o Número de Identificação Civil (NIC) dos futuros utilizadores externos da instituição e, na primeira vez que um destes utilizadores tentar aceder ao sistema, deverá validar esse número contra o que está no Cartão de Cidadão dessa mesma pessoa. Após uma validação com sucesso por CC o utilizador pode assim definir uma senha de acesso e um endereço de email, se o sistema ainda não o souber, passando assim a dispor de pelo menos dois métodos de autenticação disponíveis.

No caso de um novo utilizador desconhecido, por exemplo um candidato, o cartão permite pelo menos saber o NIC e o nome de uma forma segura, o que representa uma clara melhoria face à situação actual, em que é necessário fornecer uma conta temporária inicial e depois ter

Descrição do Problema

um processo de confirmação de identidade, antes de registar a conta definitiva. Assim pode-se passar logo à conta definitiva. Relativamente aos representantes de empresas e pessoas de outras instituições de ensino superior, uma vez que, para além do nome e do NIC, é necessário verificar a associação do CC a outras propriedades, a operação pode ser mais complexa visto que essa informação terá de ser solicitada às empresas ou instituições respectivas, o que levanta algumas questões quanto à hipótese de este número ser comunicado de forma maliciosa para uma possível personificação. É por isso importante que a instituição recolha junto da entidade externa o maior número de informações possíveis do futuro utilizador como nome completo, data de nascimento ou outros dados pessoais, sendo que estes têm de ser comunicados através de uma forma segura, como por exemplo o envio de documentos assinados de forma digital por alguém que possa ser associado com total confiança a essa mesma entidade. Neste último caso, quando o utilizador tentar aceder pela primeira vez ao SI, não só será feita uma validação do NIC mas também de todos os dados que estiverem registados na base de dados relativamente a essa pessoa.

3.2.1.2.2 Actores

- Representantes de empresas;
- Candidatos ao ensino superior;
- Pessoas de outras instituições de ensino superior.

3.2.1.2.3 Vantagens

- Maior segurança na identificação de utilizadores externos à instituição;
- Remoção da necessidade de criação de contas temporárias no SI para alguns destes utilizadores.

3.2.1.2.4 Desvantagens

É complicado extrair deste cenário desvantagens, excepto talvez o facto de que o processo de atribuição de acesso a uma pessoa externa à instituição vai passar a ser ligeiramente mais complexo, na medida em que é necessário saber pelo menos o NIC da pessoa em questão. No entanto, será consensual que neste caso, a constituição deste conjunto de etapas para a identificação de um utilizador, será uma contribuição importante para a segurança da própria Instituição.

3.2.1.2.5 Viabilidade de Implementação

Sem dúvida, uma das prioridades de implementação, tendo em conta a importância deste cenário num contexto actual de bastante insegurança e desconfiança relativamente a sistemas informáticos, com um número cada vez mais elevado de comportamentos maliciosos e de actividades fraudulentas. É de esperar que esta funcionalidade seja implementada na totalidade, estando extremamente dependente do sucesso da implementação da autenticação através do Cartão de Cidadão.

3.2.1.3 Recuperação da Senha de Acesso

Actualmente, existem milhares de milhões de páginas web na Internet e muitas delas com contas de utilizador associadas, onde o acesso ao conteúdo privado é feito por norma através da combinação do código de utilizador ou endereço email com a senha de acesso respectiva. E,

Descrição do Problema

quantas mais contas temos espalhadas pela Internet, maior é a probabilidade de nos esquecermos da combinação para uma determinada página. Existem inúmeras técnicas para recuperação da senha de acesso, mas as mais comuns passam pelo envio de um email com uma nova ou com um endereço temporário para a inserção de uma nova e pela utilização das perguntas de segurança, que mediante determinadas respostas correctas revelam ou não a senha ao utilizador.

Os sistemas da UP não são excepção ao esquecimento ou perda das senhas de acesso e, tomando como exemplo o caso da FEUP, sempre que um utilizador se esquece da senha tem duas hipóteses: escolhe receber uma senha por SMS para aceder ao SI em modo temporário para proceder à inserção de uma nova senha ou então desloca-se ao CICA e pede que lhe seja gerada uma nova senha de acesso na hora. Este último método é tão seguro como incómodo do ponto de vista que é garantida a presença física do utilizador enquanto que o primeiro, apesar de confortável e disponível a qualquer hora, é no mínimo inseguro. É esta a realidade a que se pretende acrescentar uma alternativa que combine segurança, conforto e total disponibilidade do serviço.

3.2.1.3.1 Descrição

O utilizador acede ao SI da instituição e, por múltiplas tentativas inválidas de autenticação, ou por acesso directo a uma página de recuperação da senha de acesso, o sistema deverá validar o Cartão de Cidadão disponibilizado pelo utilizador contra a informação presente na sua conta e, em caso de sucesso, será apresentado um formulário para alteração imediata da senha.

3.2.1.3.2 Actores

- Utilizadores da instituição;

3.2.1.3.3 Vantagens

- Os utilizadores deixam de se deslocar ao CICA para pedir a emissão de uma senha de acesso temporária;
- Remove a necessidade de usar um servidor de SMS para esta funcionalidade, com custos para a instituição;
- Deixa de ser necessária a intervenção de entidades externas como as operadoras móveis, o que minimiza a possibilidade de falhas alheias à própria instituição;
- Mecanismo de recuperação da senha de acesso disponível 24/7 sem custos adicionais para a instituição.

3.2.1.3.4 Desvantagens

As desvantagens deste cenário são as mesmas que as da Autenticação de Utilizadores no SI e estão essencialmente ligadas às questões físicas do CC.

3.2.1.3.5 Viabilidade de Implementação

O sucesso desta implementação está directamente ligado ao sucesso da implementação do cenário de Autenticação de Utilizadores, visto que os mecanismos de validação necessários do CC são os mesmos. Assim, está previsto que esta funcionalidade fique também implementada no decorrer do projecto e disponível para todos os utilizadores da instituição.

3.2.1.4 Preenchimento Automático de Formulários

Os dados contidos no chip do Cartão de Cidadão, permitem às aplicações informáticas o acesso a essa informação (se devidamente autorizadas pelo portador do cartão) de maneira a efectuar o preenchimento automático de formulários nas mais diversas áreas do SI. Neste caso, é de extrema utilidade o facto o cartão conter a morada do seu portador, utilizada por diversos sistemas informáticos e anda mais por aplicações ligadas ao Ensino Superior ou Sector Público em geral.

3.2.1.4.1 Descrição

Sempre que no SI surgir um formulário com dados que podem ser obtidos por leitura do Cartão de Cidadão, deverá aparecer nessa página um botão que permita ao utilizador em questão accionar um pedido de leitura aos seus dados. Após uma leitura com sucesso, o sistema pode ou não mostrar uma página (dependerá das configurações associadas à página) que contém os dados obtidos para validação do utilizador e, em seguida, esses dados serão automaticamente introduzidos nos respectivos campos do formulário.

Para que este cenário funcione com sucesso, será necessário desenhar uma arquitectura que permita um mapeamento entre os dados que podem ser obtidos do Cartão de Cidadão e os respectivos campos do formulário aos quais estes serão associados. Antes de serem inseridos os dados do cartão, deverão passar por uma camada de validação previamente definida para o formulário em questão, com funções de validação de dados respectivas para aqueles campos. Se todas as validações forem feitas com sucesso, incluindo a manual pelo utilizador, o sistema pode então proceder à passagem dos dados para o formulário.

3.2.1.4.2 Actores

- Representantes de Empresas
- Candidatos ao Ensino Superior
- Pessoas de outras Instituições de Ensino Superior
- Utilizadores da Instituição

3.2.1.4.3 Vantagens

- Dados carregados de utilizadores externos à Instituição aquando do seu registo são muito mais fidedignos quando introduzidos automaticamente pelo sistema no formulário através da sua leitura do cartão respectivo;
- Todos os documentos que necessitem de dados dos utilizadores como requerimentos ou certidões podem ser preenchidos com informação carregada directamente do cartão.

3.2.1.4.4 Desvantagens

- Complexidade de implementação da funcionalidade de maneira a que fique extremamente flexível e de fácil utilização em qualquer formulário presente no SI.

3.2.1.4.5 Viabilidade de Implementação

A relação entre a complexidade de implementação deste funcionalidade e as vantagens oferecidas pela mesma pode vir a ter um peso superior para o lado da primeira, visto que aquilo que é necessário desenvolver para que este cenário se torne possível, na sua forma mais

Descrição do Problema

completa, pode por em causa os benefícios que disponibiliza aos utilizadores da Instituição. Uma possível abordagem será o desenvolvimento de casos concretos de preenchimento automático de formulários, como a actualização de dados na área de gestão pessoal dos utilizadores ou o registo de utilizadores externos à Instituição. Esta decisão será tomada ao longo da duração do Projecto e está dependente do sucesso e rapidez com que funcionalidades de maior prioridade sejam implementadas.

3.2.1.5 Controlo de Acessos

Os alunos e funcionários da FEUP acedem, neste momento, às instalações da Instituição através do cartão que é atribuído a cada um destes elementos, tal como é feito o acesso aos parques de estacionamento.

3.2.1.5.1 Descrição

Quando um aluno, funcionário ou outro cidadão externo à instituição, se deslocam a um ponto de acesso de um determinado recurso e, após a introdução do Cartão de Cidadão no leitor, o sistema deverá verificar se a pessoa tem permissões para aceder ao recurso. Este cenário pode permitir à Instituição a substituição dos actuais cartões pela utilização do Cartão de Cidadão.

3.2.1.5.2 Actores

- Utilizadores da instituição;
- Outros cidadãos que necessitam de entrar nas instalações da instituição.

3.2.1.5.3 Vantagens

- Elimina a produção de cartões para todos os membros e permite à instituição poupar dinheiro e logística em todo o processo que está associado ao actual mecanismo de controlo de acessos;
- Sempre que algum convidado ou outra entidade se deslocar às instalações da instituição através de um veículo automóvel poderá colocar a viatura no parque de estacionamento se tiver sido previamente autorizado.

3.2.1.5.4 Desvantagens

- Os alunos da instituição perdem a identificação enquanto estudantes universitários;
- Necessidade de substituir os leitores de banda magnética actualmente utilizados para os cartões da instituição por leitores de SC em todos os pontos de acesso da instituição (salas, departamentos, parques de estacionamento, ...);
- Decisão de substituição do cartão na instituição depende da opinião de diversas pessoas com nível de decisão hierarquicamente superior e de vários interesses associados à permanência do actual sistema de cartões da instituição.

3.2.1.5.5 Viabilidade de Implementação

A implementação deste cenário pode não ser possível, por uma série de factores alheios à própria Instituição e às mudanças que o novo sistema implicaria em toda a estrutura do controlo de acessos, mas, é importante estudar esta possibilidade e preparar toda uma estrutura de

Descrição do Problema

suporte às funcionalidades associadas à utilização do Cartão de Cidadão como identificador para acesso às instalações da instituição.

Um contacto informal junto da CNPD permitiu concluir que, embora a utilização do CC para acesso à entrada principal da instituição pudesse ser considerada, se considerava excessiva a utilização do CC para acesso a espaços interiores, como salas, laboratórios, parques, etc.

3.2.1.6 Controlo da Assiduidade

Dentro deste cenário é necessário considerar duas abordagens: o controlo da assiduidade dos funcionários da instituição para efeitos de recursos humanos e responsabilidades para com a entidade patronal e o controlo da assiduidade dos alunos da instituição em aulas e outros eventos de frequência obrigatória para efeitos académicos.

3.2.1.6.1 Descrição

No que diz respeito ao controlo da assiduidade dos funcionários, neste momento a Instituição possui um sistema bastante avançado para o efeito e uma nova implementação passaria apenas pela substituição do actual cartão de colaborador da instituição pelo Cartão de Cidadão de cada pessoa. Neste cenário, o sistema deixaria de guardar as impressões digitais dos funcionários e passaria a validar apenas os dados biométricos contidos no cartão contra a impressão digital do colaborador que se está a tentar autenticar.

3.2.1.6.2 Actores

- Utilizadores da instituição;

3.2.1.6.3 Vantagens

- Os utilizadores da instituição deixam de poder marcar presença tanto a nível de aulas como no posto de trabalho a outros colegas;
- A recolha de todos estes dados por parte da instituição permite-lhe gerar estatísticas fidedignas daquilo que realmente acontece a nível de presença em aulas e outros eventos académicos com relevância;
- Deixa de ser necessário recolher as impressões digitais dos utilizadores da instituição e lidar com os problemas, que no caso dum ambiente académico podem ser alguns milhares de novas impressões por ano;
- Instituição deixa de possuir uma base de dados de impressões digitais, retirando as questões éticas que estão associadas à utilização deste tipo de aplicações e removendo um sentimento de insegurança quanto à possibilidade da informação ser acedida maliciosamente por terceiros.

3.2.1.6.4 Desvantagens

- Seria necessário a aquisição de algumas centenas de equipamentos de leitura de dados biométricos para os colocar em todas as salas de aula e outras instalações onde seja necessário controlar a presença das pessoas respectivas;
- Aplicação actual de controlo da assiduidade presente na instituição é recente e representou um investimento bastante grande, logo a sua substituição não seria consensual e muito menos seria feita num futuro próximo;

Descrição do Problema

- É preciso ter em atenção as restrições impostas pela Comissão Nacional de Protecção de Dados (CNPD) quanto ao uso do CC para fins ligadas a empresas porque, segundo eles, o cartão foi criado para um relacionamento entre o cidadão e o Estado.

3.2.1.6.5 Viabilidade de Implementação

Além de toda a controvérsia legal à volta deste cenário, será também de longe o mais complexo de implementar no âmbito do projecto. Não só porque existe muito pouca informação disponível sobre a utilização do mecanismo de validação por impressão digital e a que existe não é coerente (algumas entidades dizem que este tipo de autenticação só está disponível para as autoridades judiciais enquanto outras afirmam que é um mecanismo aberto), mas também porque envolve o uso de mais dispositivos externos com ligação aos recursos humanos. Apesar da inovação da funcionalidade, tendo em conta o tempo limitado e a falta de recursos e referências, a opção passa por a colocar no fundo da lista das implementações.

3.2.2 Assinatura Digital

Uma das maiores inovações que o Cartão de Cidadão proporciona é a inclusão de um certificado digital ou assinatura digital como é por vezes referido, que permite aos cidadãos selarem um determinado conteúdo com a sua assinatura de forma digital. Assim que o conteúdo for alterado, pelos próprios ou terceiros, essa assinatura é automaticamente removida do conteúdo a que tinha sido associada previamente. É neste contexto que se pretende expandir esta funcionalidade a outras áreas do SI e a outras aplicações em geral.

3.2.2.1 Assinatura de Documentos

À semelhança de uma assinatura manual que tem como finalidade identificar a pessoa ou a entidade responsável pela emissão de um documento em papel, a assinatura digital tem como intuito assinar documentos electrónicos e identificar a sua origem. Existem alguns manuais disponibilizados pela AMA que explicam como inserir a assinatura digital do Cartão de Cidadão num documento criado através do Microsoft Word, OpenOffice.org ou Adobe Acrobat mas este cenário pretende expandir este conceito a documentos internos do SI.

3.2.2.1.1 Descrição

Se tivermos em consideração um ambiente académico onde existe uma constante troca de informação sensível entre os membros da instituição, como, por exemplo, classificações das disciplinas, actas de reuniões, pedidos de despesas e outros documentos importantes, é de extrema importância que as pessoas envolvidas possam confiar na origem desses documentos. Se, por exemplo, a secretaria central da instituição recebe as classificações finais de uma disciplina, então os seus funcionários devem ter a certeza que efectivamente esse documento foi enviado pelo responsável dessa mesma disciplina ou por quem tem permissões para o fazer. Esta troca de informação pode ocorrer através de mensagens electrónicas, acesso a ficheiros no SI ou até através de dispositivos de armazenamento de dados como CD's ou DVD's, mas o importante aqui é que os documentos em si estejam assinados digitalmente.

3.2.2.1.2 Actores

- Utilizadores da instituição.

3.2.2.1.3 Vantagens

- Se um documento for assinado digitalmente o destinatário pode confiar na sua origem, i.e., o documento foi criado por quem o assinou e este não o pode negar (não-repúdio);
- Os membros da instituição não têm de se deslocar em pessoa a outros departamentos ou escritórios de maneira a entregar em mão um documento;
- O mesmo documento pode circular entre várias pessoas e ser alterado várias vezes e a assinatura digital pode ser adicionada a cada alteração, ao contrário do modelo de papel, onde cada alteração implica que o documento tenha de ser impresso e todos os autores têm de assinar novamente, ou então, o texto adicionado ou alterado tem de estar bem especificado, o que nem sempre é facilmente realizável.

3.2.2.1.4 Desvantagens

- O mecanismo de assinatura digital de um documento, no momento em que este é carregado para a base de dados, tem algumas restrições tecnológicas e isso pode criar algumas limitações nos sistemas operativos ou navegadores suportados.

3.2.2.1.5 Viabilidade de Implementação

Esta funcionalidade é extremamente importante no âmbito da dissertação e sobre aquilo que representam as novas potencialidades do Cartão de Cidadão. Se por um lado a assinatura digital de documentos externos ao SI é bastante fácil, pelo menos com um número limitado de aplicações, a assinatura de documentos no momento em que são inseridos na base de dados pode ser bastante complexa de implementar muito devido às limitações da Oracle e do acesso aos certificados no CC. Contudo, existem alguns estudos neste campo e esta funcionalidade está no topo da lista das implementações por isso está previsto pelo menos uma versão inicial.

3.2.2.2 Assinatura de Mensagens Electrónicas

Tal como no cenário anterior, também para a assinatura de mensagens electrónicas existem uma série de documentos explicativos da AMA para a integração das duas ferramentas de email mais conhecidas do mercado, o Microsoft Outlook e o Mozilla Thunderbird. Ao contrário do que acontece no cenário da assinatura de documentos, os emails não são armazenados na base de dados associada ao SI da instituição mas antes são enviados através de servidores dedicados. Seria interessante perceber, durante a dissertação, se esses servidores podem ser manipulados de alguma forma, de maneira a integrar automaticamente a assinatura das mensagens enviadas com o Cartão de Cidadão. Pode também ser analisada uma solução para a implementação da solução na versão web do mail, independente do SI da instituição.

3.2.2.2.1 Descrição

O contexto das mensagens electrónicas assinadas digitalmente é em muito semelhante ao caso anterior dos documentos. Também aqui se coloca em causa a troca de informação sensível entre elementos da instituição, onde é extremamente importante ter a certeza se o remetente de uma mensagem é quem o diz ser. As implicações de segurança são idênticas ao cenário anterior e as maiores diferenças prendem-se com as implicações e limitações tecnológicas associadas à sua implementação com o CC.

Descrição do Problema

3.2.2.2.2 Actores

- Utilizadores da instituição.

3.2.2.2.3 Vantagens

- Se uma mensagem electrónica for assinada digitalmente, o destinatário pode confiar na sua origem, i.e., a mensagem foi criada por quem o assinou e este não o pode negar (não-repúdio);
- No caso de sucesso de uma implementação, integrada de alguma forma com os servidores de mail da instituição, a solução é completamente transparente para os utilizadores e evita uma série de constrangimentos com as aplicações de mail existentes.

3.2.2.2.4 Desvantagens

- A implementação da solução integrada pode não ser possível, ou o tempo e recursos envolvidos podem por em causa a sua implementação, mas a versão mais básica do cenário com a utilização de aplicações externas continua a ser uma realidade.

3.2.2.2.5 Viabilidade de Implementação

Ao longo da descrição deste cenário de utilização, foi chamada a atenção para os problemas associados à tentativa de implementação de uma solução integrada e inovadora nos servidores de mail da instituição, mas como foi mencionado, tal pode não ser possível e este mecanismo não está no topo das prioridades de implementação no contexto desta dissertação. No pior dos cenários, a utilização da assinatura do CC nas mensagens electrónicas pode ser feita com as aplicações de mail existentes no mercado.

3.2.2.3 Assinatura de Conteúdos da Base de Dados

Além dos documentos que podem vir a ser assinados com o CC no momento de inserção na base de dados ou externamente assinados e depois inseridos, é também interessante estudar a possibilidade de implementação da assinatura de dados dentro de colunas ou registos completos da base de dados. Esta assinatura pode ser associada a um campo de uma tabela em específico ou a um conjunto de registos de diferentes tabelas que agregados compõem um objecto válido. É um factor de inovação, na medida em que, a maior parte das soluções implementadas com as assinaturas digitais do CC visam maioritariamente os documentos, enquanto que esta transporta este modelo para dentro de uma base de dados.

3.2.2.3.1 Descrição

Comparativamente com a informação armazenada, por exemplo, num banco, pode-se dizer que os conteúdos disponibilizados num ambiente académico são menos sensíveis do ponto de vista de repercussões sobre a falsidade de dados apresentados. E, se esta afirmação é de facto verdadeira, também o é que não deixa de existir informação importante neste tipo de instituições e que esta não pode ser posta em causa.

Alguns exemplos de conteúdos importantes na base de dados institucional são, por exemplo, as notas de uma disciplina e conteúdos de mensagens transmitidas entre elementos da direcção com um carácter de decisão administrativa. Imaginemos que, a determinada altura do ano lectivo, o professor responsável de uma disciplina lança as notas para publicação e, tendo em conta que essa informação é armazenada na base de dados, quem nos garante que foi

Descrição do Problema

efectivamente esse professor que inseriu esse conteúdo? E se esses dados tiverem sido manipulados por alguém de maneira a que pareçam terem sido criados pelo professor? E, se no segundo exemplo referido atrás, um funcionário receber uma notificação do director da faculdade para executar uma tarefa que na realidade não tenha sido enviada por ele, mas sim por alguém com interesses maliciosos? São este tipo de questões que podem causar problemas graves e de consequências devastadoras não só para os destinatários, mas também para aqueles que viram a sua identidade falsificada. É neste contexto, que um sistema de informação cada vez mais repleto de funcionalidades mas também responsabilidades, deve garantir aos seus utilizadores que a origem de dados sensíveis não pode ser posta em causa.

3.2.2.3.2 Actores

- Utilizadores da instituição.

3.2.2.3.3 Vantagens

- Confiança na origem do conteúdo dos dados armazenados na base de dados;
- Possibilidade de múltiplos autores (assinantes) sobre o mesmo conteúdo, como por exemplo no caso de actas de reuniões onde o documento é só um mas existem várias pessoas que assinam.

3.2.2.3.4 Desvantagens

- Os dados estão a ser armazenados de uma determinada forma neste momento pelo que uma alteração deste género pode ser estruturalmente complexa.

3.2.2.3.5 Viabilidade de Implementação

Dentro do área da assinatura digital é sem dúvida o mais complexo a nível de arquitectura e implementação, mas é também um ponto de extremo interesse para o SI pelo que será dada a devida importância na lista de prioridades a implementar. No entanto, na implementação deste cenário poderão existir conflitos com o sistema actual de armazenamento de informação pelo que o mecanismo tem que ser bem estruturado sem pôr em causa as funcionalidades anteriores do SI para a sua implementação.

3.2.3 Encriptação

Infelizmente, não faz parte do Cartão de Cidadão uma estrutura de suporte à encriptação de dados, visto que este não possui um certificado digital para esse efeito. No entanto, existem soluções alternativas que podem ser implementadas com uma estrutura intermédia entre o SI e o CC. O custo de implementação de uma estrutura do género é bastante superior aos mecanismos descritos anteriormente para a autenticação e assinatura digital, mas o ganho tecnológico justifica por si só o esforço que se possa vir a fazer nesse sentido. A presente secção descreve cenários de utilização dos mecanismos de encriptação num ambiente académico, independentemente da estrutura vir a ser ou não implementada na instituição.

3.2.3.1 Encriptação de Documentos

Se a validade da origem de uma determinada informação (assinatura digital) é um factor de extrema importância no estabelecimento de uma relação de confiança entre um SI e o seus

Descrição do Problema

utilizadores, também a confidencialidade dessa informação representa um papel importante em muitos casos. Uma assinatura digital num documento garante que este não foi alterado desde que foi assinado até ao momento em que chegou ao destino, mas não nos garante que não foi interceptado e visualizado por outros intervenientes entretanto. É aqui que entram as funções de encriptação de dados e neste caso em concreto, a encriptação de documentos.

3.2.3.1.1 Descrição

Mais uma vez, e tal como no caso da assinatura de documentos, existem duas abordagens diferentes ao problema da encriptação de documentos: aqueles que são criados em ferramentas externas ao SI e enviadas aos seus destinatários sem nunca passarem pelo sistema e os outros que apesar de terem sido criados externamente podem ser armazenados no SI e a sua consulta disponível para os respectivos intervenientes desejados. Em qualquer dos cenários a chave para desencriptação do documento tem de ser enviada aos destinatários de alguma forma, pelo que a maneira mais segura de o fazer é através do SI e da sua estrutura de encriptação intermédia para o Cartão de Cidadão.

3.2.3.1.2 Actores

- Utilizadores da instituição.

3.2.3.1.3 Vantagens

- Privacidade e confidencialidade nos documentos transmitidos a outros utilizadores;
- Utilização das capacidades do CC juntamente com as funcionalidades de encriptação;

3.2.3.1.4 Desvantagens

- A necessidade de uma camada intermédia para fazer a encriptação através do CC;
- Na transmissão da chave assimétrica aos destinatários pode não ser possível garantir a segurança desejada.

3.2.3.1.5 Viabilidade de Implementação

Toda a componente da encriptação está directamente ligada à estrutura de encriptação intermédia sobre o CC, logo o sucesso de implementação deste cenário depende também da rapidez com que essa estrutura seja desenvolvida e quais os mecanismos suportados pela mesma. Embora estejam aqui descritos, no mesmo cenário, os documentos encriptados criados e enviados externamente ao SI e os documentos encriptados armazenados na base de dados, estes devem ser tratados de maneira diferente na questão da prioridade de implementação, sendo que tudo o que está relacionado directamente com o SI tem prioridade sobre o resto.

3.2.3.2 Encriptação de Mensagens Electrónicas

Tão importante como a encriptação de documentos, a encriptação de mensagens representa um papel fundamental na comunicação dentro e fora de qualquer instituição. Cada vez mais, os cidadãos e utilizadores em particular, exigem maior privacidade na sua vida e naquilo que fazem e desde que não prejudiquem ninguém no processo, têm todo o direito de o fazer. Além da questão da privacidade pessoal, existe também a importância da confidencialidade, dentro de

Descrição do Problema

uma instituição, dos dados enviados por email a outras pessoas. Se a comunicação electrónica é cada vez mais comum e essencial, então a instituição deve também garantir a satisfação das condições mencionadas num ambiente digital.

3.2.3.2.1 Descrição

No caso concreto da UP, a encriptação de mensagens electrónicas seria maioritariamente feita em aplicações externas ao SI, pelo que seria necessário criar um mecanismo de integrar o sistema com as diversas aplicações existentes no mercado para o envio de emails. O processo de encriptação seria semelhante ao do utilizado na encriptação de documentos, com a excepção que o SI não armazenaria nenhum tipo de informação sobre o email, tirando os acessos à chave simétrica. Outra abordagem ao problema passa por definir, como no contexto das assinaturas, mecanismos de ligação dos servidores de mail ao SI de maneira a que as mensagens sejam encriptadas, no momento de envio, e os respectivos acessos gerados automaticamente na base de dados.

3.2.3.2.2 Actores

- Utilizadores da instituição.

3.2.3.2.3 Vantagens

- Confidencialidade nas mensagens enviadas a outros cidadãos;
- Em caso de sucesso na integração da estrutura de encriptação com os servidores de mail, a ferramenta será uma mais valia a todos os níveis, sem necessidade de intervenção manual do utilizador quando quer encriptar uma mensagem para outro utilizador.

3.2.3.2.4 Desvantagens

- Além das desvantagens do cenário anterior, a integração com os servidores de mail pode não ser possível ou os recursos necessários serem demasiado extensos.

3.2.3.2.5 Viabilidade de Implementação

Apesar de não ser uma funcionalidade vital, representa, sem dúvida, uma mais valia com bastante inovação dentro da instituição e, desde que seja atingido sucesso na implementação do cenário anterior, também este deve ser passível de implementação. A prioridade da versão mais básica deste conjunto de procedimentos é estar à frente da integração da estrutura de encriptação com os servidores de mail da instituição.

3.2.3.3 Encriptação de Conteúdos da Base de Dados

Se a encriptação da informação armazenada numa base de dados não é uma inovação, a encriptação desses dados através de uma estrutura de encriptação com o CC e o armazenamento posterior, é. Infelizmente, o módulo de segurança avançada da Oracle não pode ser suportado financeiramente e, consequentemente, não podemos utilizar as potencialidades da encriptação transparente de dados previstas pela empresa para a sua base de dados, pelo que as alterações necessárias para qualquer outra abordagem ao problema serão sempre consideráveis e é algo que devemos ter em conta na implementação da solução.

3.2.3.3.1 Descrição

Actualmente, o SI armazena na base de dados diversas informações associadas às mais distintas áreas da instituição. Se por um lado, muitos desses dados são públicos como, por exemplo, os planos de estudo ou as listagens de alunos e funcionários, por outro lado existe também muita informação privada apenas destinada a pessoas ou grupos de utilizadores específicos como, por exemplo, o percurso académico de um aluno que está só disponível para o próprio estudante ou para aqueles que se encarregam da gestão dessa informação. É este o tipo de funcionalidades que se pretende que sejam implementadas no sistema e que sejam tornadas disponíveis para os utilizadores do SI.

3.2.3.3.2 Actores

- Utilizadores da instituição.

3.2.3.3.3 Vantagens

- Confidencialidade da informação armazenada na base de dados do SI;
- Garantia que só as pessoas indicadas pelo utilizador conseguem visualizar os dados armazenados, sendo que nem o próprio administrador da base de dados o consegue.

3.2.3.3.4 Desvantagens

- Além das desvantagens do primeiro cenário associado ao uso de encriptação, a complexidade da estrutura de suporte a uma solução destas;
- Taxa de crescimento da lista de acessos a determinados registos da base de dados muito elevada, se tivermos em conta que as pessoas com permissões para visualização podem ser todos os membros de um grupo com centenas de utilizadores.

3.2.3.3.5 Viabilidade de Implementação

Sem dúvida um desafio de implementação com uma componente de inovação enorme mas também com aplicações extremamente importantes na instituição. No entanto, é preciso analisar as vantagens do cenário contra as suas desvantagens e o tempo de desenvolvimento associado, pelo que a prioridade de implementação destes mecanismos também passa muito no sucesso da implementação da estrutura de encriptação.

3.3 Resumo

Ao longo deste capítulo foram apresentados possíveis cenários de utilização do Cartão de Cidadão no ambiente académico da UP em geral e da FEUP em particular. Ambiente académico não significa ambiente sem responsabilidades legais e morais para com os seus utilizadores e pessoas externas à instituição, na medida em que é necessária muita atenção na implementação da solução aos pormenores de segurança e confidencialidade da informação tratada, enviada e armazenada. Esta é uma relação de confiança que a instituição tem de construir com os seus utilizadores através da disponibilização de mecanismos em que estes confiem.

Foi possível perceber também a complexidade associada à implementação de muitas destas funcionalidades e do esforço necessário para as atingir. De realçar a possível criação de uma estrutura de encriptação intermédia com o Cartão de Cidadão na própria instituição e a estrutura

Descrição do Problema

para a inserção de assinaturas digitais sobre registos múltiplos da base de dados, como soluções que imprimem um carácter de bastante inovação à dissertação.

4 Solução Proposta

Neste capítulo são descritas as decisões tomadas a nível de arquitectura e implementação das funcionalidades listadas no capítulo anterior. São também apresentadas as limitações que foram sendo impostas ao longo do projecto, tanto ao nível de custo de desenvolvimento como também devido ao sistema existente e à sua integração com os mecanismos desejados. Foram incluídos no seu conteúdo todos os cenários de uso e respectiva modelação, não tendo em conta o esforço de implementação, que será ilustrado no capítulo 5.

4.1 Introdução

A complexidade de algumas das funcionalidades apresentadas no capítulo anterior como parte de uma lista de casos de uso, juntamente com a diversidade de aspectos tecnológicos a ter em conta na sua implementação em campos distintos como a criptografia, o armazenamento de dados, a utilização multi-plataforma de dispositivos de segurança e o uso de aplicações externas em conjunto com o sistema a implementar, pode tornar as soluções pouco elucidativas e sujeitas a erros graves de estruturação. Ao longo desta fase de tomada de decisões, as funcionalidades a implementar foram divididas em diferentes áreas de utilização do Cartão de Cidadão no SI. Para cada uma das áreas foram apresentadas soluções do ponto de vista técnico que permitem, não só a sua implementação imediata, mas também a abertura a futuras alterações tendo em conta a previsão da evolução de algumas tecnologias, dentro do que é possível antecipar.

Nas soluções analisadas ao longo deste capítulo estão presentes especificações de diversas áreas de intervenção, desde estruturas para a base de dados, configurações a efectuar tanto no servidor aplicacional como no de base de dados, lógica de negócio de funcionamento dos casos de uso, estrutura do código a implementar e definição de uma API para integração com muitas áreas do SI. Todas estas especificações irão fazer parte de um módulo genérico que decorre do estudo efectuado neste dissertação, o Módulo de Segurança Avançada (MSA), e dentro desse módulo estarão outras componentes específicas aos cenários de utilização, como é descrito na Arquitectura.

4.2 Autenticação

Se por um lado a introdução da autenticação com recurso a *smart cards* é uma aposta forte da instituição nos novos mecanismos de segurança em sistemas de informação, por outro lado as implicações que derivam dessa funcionalidade também podem trazer algum constrangimento à instituição e aos seus utilizadores: à instituição porque tem de assegurar aos seus membros uma cobertura considerável de acesso a leitores de dispositivos deste tipo, porque se os recursos de acesso forem limitados poucos serão os utilizadores que por iniciativa pessoal, se irão munir desses dispositivos no local de trabalho; aos utilizadores porque, tratando-se de um documento de cidadania que contém bastante informação pessoal, a instituição tem de garantir o não acesso a esses dados por terceiros ou que essa informação seja de alguma forma espalhada sem o consentimento do cidadão em causa.

Financeiramente, pelo menos a curto prazo, pode ser inviável uma cobertura total de todos os pontos de acesso na UP com leitores do CC, mas seria interessante disponibilizar esse tipo de dispositivos para os elementos da direcção e talvez da administração central, sendo estes os utilizadores que lidam normalmente com informação mais sensível dentro da instituição. A título pessoal, a aquisição de leitores é uma possibilidade para muita gente tendo em conta que não estamos a falar de valores astronómicos, mas não podemos julgar as finanças das pessoas que fazem parte da instituição. Por isso, o importante é pensar na realidade dentro da UP e com recursos disponibilizados pela instituição.

4.2.1 Autenticação de Utilizadores

Para a implementação do cenário descrito na secção 3.2.1 e considerando as barreiras das tecnologias impostas, existem duas abordagens possíveis: usar o servidor aplicacional (Apache) para efectuar a validação dos certificados de autenticação presentes do CC dos utilizadores ou implementar uma solução de autenticação usando uma applet em Java que faz o acesso aos mesmos certificados. Em ambos os casos, após o pedido dos certificados de autenticação do CC dos utilizadores, os certificados são enviados para o servidor da base de dados de maneira a poder efectuar a validação do utilizador em concreto que está a tentar aceder ao sistema.



Figura 4.1: Logotipo do Apache

Após alguma deliberação sobre o caminho a seguir, optámos pela utilização do Apache como intermediário entre os certificados do utilizador e a base de dados. As vantagens desta opção passam por um menor esforço de implementação, visto que o Apache tem os mecanismos necessários implementados para este tipo de autenticação, e por questões de compatibilidade e esforço mínimo nos navegadores dos utilizadores do SI, tendo em conta que a utilização de Java na Web não está completamente uniformizada e por vezes os comportamentos são difíceis de

prever. Ao contrário dos outros cenários descritos ao longo desta dissertação, em que o problema de não funcionarem com determinadas versões de navegadores ou sistemas operativos pode ser aceitável, é sem dúvida fundamental que esta funcionalidade seja transversal a todas as aplicações e utilizadores.

4.2.1.1 Requisitos

A autenticação com certificados digitais no Apache implica uma série de instalações extra e um conjunto bastante grande de configurações a fazer no servidor. Implica também um leque de conceitos associados às autoridades de certificação e à validade ou revogação dos certificados. No que diz respeito aos utilizadores, estes não tem de fazer nenhuma instalação ou configuração extra nas suas máquinas, à excepção daquelas que são necessárias para a utilização do CC em geral, como definido pela AMA.

Para que se consiga implementar um mecanismo de autenticação no Apache com o CC, é necessário instalar antes de mais o OpenSSL no servidor em questão e é preciso adquirir ou criar localmente um certificado para o próprio servidor, sendo que o criado localmente fica inválido e gera uma séria de mensagens de erro para os utilizadores. Isto porque esta funcionalidade só pode ser efectuada através de uma ligação segura entre o navegador e a máquina (SSL), com um certificado devidamente autorizado por uma autoridade de certificação válida ou então desde que utilizador assuma os riscos e aceite no seu computador um certificado inválido. Actualmente a FEUP e a maior parte das instituições da UP possuem certificados SSL válidos por isso esta não é uma questão impeditiva.

É ainda necessário instalar no servidor todos os certificados associados às EC do Cartão de Cidadão e do Estado, desde as três entidades responsáveis pela assinatura dos certificados de autenticação, passando pela EC do CC que os assina, até à EC raiz do Estado, por sua vez assinada por uma autoridade de certificação de confiança global e comum a todos os sistemas operativos. Só assim se consegue garantir que o Apache reconhece os certificados presentes no CC e procede à validação dos utilizadores, mas antes da instalação é preciso converter todos os certificados do formato CER disponibilizado pelas entidades competentes, para o formato PEM utilizado pelo OpenSSL e reconhecido como um formato mais aberto que o anterior.

4.2.1.2 Estrutura de Dados

Antes de avançarmos para uma definição da estrutura de dados necessária para suportar a autenticação de utilizadores no SI, é importante percebermos a maneira como a informação está neste momento na base de dados actual de utilizadores e como funciona a autenticação do sistema. Tal como foi introduzido no capítulo de Enquadramento Tecnológico do Estado da Arte, o GESSI é responsável pela gestão dos mecanismos de autenticação enquanto que a informação detalhada dos utilizadores é mantida no SI da instituição, neste caso o SIGARRA. A ligação entre ambos é feita com uma associação da tabela LOGINS do GESSI com a tabela PESSOAS do SI através do código do utilizador, que no caso do SIGARRA é normalmente o código de funcionário ou estudante da instituição. É importante mencionar também que, do ponto de vista técnico, o GESSI e o SIGARRA são duas aplicações independentes, instaladas em esquemas distintos mas na mesma instância da base de dados.

As implementações de novas funcionalidades para um sistema em produção devem sempre minimizar o custo de adaptação do sistema existente, de forma a que as alterações a efectuar na estrutura da aplicação sejam apenas as essenciais, sem nunca colocar em causa o que antes estava a funcionar. É com este pensamento em mente que vamos definir uma estrutura flexível e

o mais independente possível da situação actual das aplicações, que pode ser adicionada como uma funcionalidade extra ao SI a qualquer momento sem problemas com dependências ou conflito de versões das diferentes aplicações. Na figura 4.2 podemos ver uma versão simples do modelo de dados que está associado ao que foi descrito sobre a autenticação de utilizadores (o diagrama não mostra a listagem completa das colunas das tabelas, mas ilustra apenas a lógica entre as mesmas e a estrutura de suporte à funcionalidade).

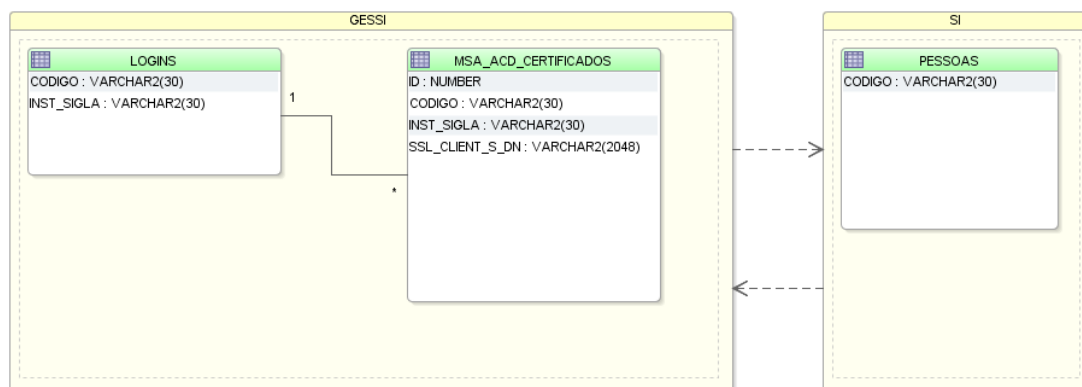


Figura 4.2: Estrutura de Dados para a Autenticação de Utilizadores

Como podemos ver na figura acima, a tabela MSA_ACD_CERTIFICADOS é o elemento responsável pela ligação entre as duas aplicações e mais concretamente entre utilizadores e pessoas (explicação sobre a nomenclatura adoptada pode ser vista mais à frente neste capítulo na Arquitectura e no capítulo sobre Implementação). Além de independente do sistema existente, esta estrutura foi também pensada para suportar outro tipo de certificados digitais que não os do Cartão de Cidadão de maneira que a coluna SSL_CLIENT_S_DN da tabela pode ser usada com expressões regulares. No caso concreto do CC e de maneira a que a autenticação funcione com este método, o campo será preenchido por exemplo com `^.*serialNumber=BI123278155[.]*$`, em que a aplicação irá validar o campo DN do certificado fornecido na autenticação com essa expressão regular.

4.2.1.3 Modo de Funcionamento

O primeiro passo para a utilização do CC como método de autenticação é a associação da conta do utilizador, pelo próprio, ao seu cartão, isto é, antes de utilizar pela primeira vez este serviço o utilizador deve configurar o acesso no sistema de maneira a que o SI consiga associar o seu cartão a uma conta existente. No que diz respeito ao sistema, esta associação não é mais que uma pesquisa na lista de utilizadores e pessoas associadas pelo NIC indicado no CC e a consequente inserção na tabela MSA_ACD_CERTIFICADOS da ligação entre o certificado e a conta de utilizador respectiva.

Uma vez a associação feita, o acesso ao SI com o CC deve ser feito com o conhecimento do cidadão de tal forma que, segundo as normas da AMA para a utilização em ambientes Web deste tipo de autenticação, deve ser mostrada na página de acesso ao CC uma referência clara a este facto, quer através de uma imagem ou de texto bem explícito. Depois de concordar com o acesso ao certificado e em caso de sucesso de validação do mesmo, o sistema deve iniciar uma sessão de autenticação da mesma forma que é feita actualmente e essa informação armazenada na base de dados por questões de segurança e histórico de acessos.

4.2.2 Identificação de Pessoas Externas

Não existem grandes novidades a nível de implementação neste caso de uso, relativamente ao de Autenticação de Utilizadores, e as questões a ter em conta aqui prendem-se mais com a forma como estes utilizadores são registados no sistema pelos funcionários competentes. Neste momento, as entidades externas ao SI são registadas através de contas temporárias com códigos de utilizador e senhas de acesso geradas automaticamente pelo sistema, sendo depois estes dados transmitidos à entidade em questão para posterior autenticação no sistema.

Esta funcionalidade não apresenta alterações estruturais à solução em questão e as únicas modificações que serão necessárias fazer implicam apenas que na estrutura exista um método para definir contas temporárias à espera de activação com o respectivo Cartão de Cidadão. Outra implementação necessária, inserida neste cenário, é um formulário intermédio de inserção de uma senha de acesso e um que permita ao utilizador completar os seus dados pessoais em falta depois de devidamente autenticado.

4.2.2.1 Requisitos

Nada a acrescentar aos requisitos listados na secção 4.2.1.1 para suporte à implementação da funcionalidade de Autenticação de Utilizadores.

4.2.2.2 Estrutura de Dados

Nada a acrescentar à estrutura apresentada na secção 4.2.1.2 para apoio à implementação da funcionalidade de Autenticação de Utilizadores.

4.2.2.3 Modo de Funcionamento

Analisando o caso em concreto dos elementos externos nomeados para júris responsáveis pela avaliação de teses e dissertações elaboradas pelos estudantes da instituição, é fácil perceber que esses utilizadores têm de ser registados no sistema de maneira a poderem aceder ao SI para consulta de várias páginas ou documentos importantes, por exemplo. Neste novo cenário, o registo destes elementos é feito na altura da nomeação para o júri, devidamente associados à respectiva instituição externa, de forma que, assim que estes utilizadores acederem ao SI pela primeira vez, o sistema automaticamente irá requisitar o certificado de autenticação do cidadão em questão e, em caso, de sucesso no processo de validação do mesmo, será redirecionado para um formulário onde tem de introduzir a sua senha de acesso e, se for caso disso, completar informação pessoal em falta. No final do processo, o sistema pode então confiar na identidade do utilizador e a autenticação por CC em acessos posteriores fica ao critério do mesmo.

4.2.3 Recuperação da Senha de Acesso

Tal como no cenário anterior, também a recuperação da senha de acesso não implica uma alteração sobre aquilo que foi feito para o caso de uso de Autenticação de Utilizadores. Este caso é tão semelhante do ponto de vista técnico com o anterior que têm em comum o mesmo formulário para inserção de uma nova senha de acesso para a conta de utilizador, sendo que neste cenário concreto a conta do utilizador está activa ou bloqueada no caso de múltiplas tentativas inválidas de autenticação.

4.2.3.1 Requisitos

Nada a acrescentar aos requisitos listados na secção 4.2.1.1 para suporte à implementação da funcionalidade de Autenticação de Utilizadores.

4.2.3.2 Estrutura de Dados

Nada a acrescentar à estrutura apresentada na secção 4.2.1.2 para apoio à implementação da funcionalidade de Autenticação de Utilizadores.

4.2.3.3 Modo de Funcionamento

O modo de funcionamento deste cenário é bastante semelhante ao dos dois cenários acima descritos a nível da interacção com o SI, na medida em que pelo desconhecimento da sua senha de acesso ou por bloqueio de conta, os utilizadores do sistema recorrem a uma página desenhada para o efeito e podem-se autenticar com o CC e posteriormente efectuar a troca da sua senha de acesso. No entanto, neste caso em concreto há que ter em atenção que o utilizador pode nunca ter usado este tipo de autenticação previamente, caso em que a sua configuração não estará inserida no sistema. Uma verificação adicional é então necessária e o SI deve proceder de acordo com o seu resultado.

4.2.4 Preenchimento Automático de Formulários

Tecnologicamente o cenário mais complexo de implementar na área de autenticação com o CC, o preenchimento automático de formulários pode ser efectuado de diferentes maneiras: com uma página intermédia de acesso aos dados do CC previamente definidos e que depois são submetidos para um procedimento especificado; com recurso a funções da API que incluam num determinado formulário uma componente de acesso aos dados do CC que são submetidos em conjunto com o resto dos campos do formulário principal; com uma chamada AJAX a uma página para o efeito único de leitura dos dados pessoais do cidadão a qual depois retorna os valores obtidos para a página que origina a chamada em tempo real.

Em qualquer dos casos, do ponto de vista de implementação, o mais importante não é maneira como o acesso aos dados é mostrado, mas sim a maneira como é feita a ligação a essa extracção de dados do CC. Ainda no último caso da utilização de uma chamada AJAX, seria muito interessante do ponto de vista de desenvolvimento a capacidade de, consoante um grupo de palavras pré-definidos como por exemplo morada, endereço ou código postal, poder detectar automaticamente a possível presença num determinado formulário de dados passíveis de serem obtidos directamente do Cartão de Cidadão, à semelhança das soluções desenvolvidas em aplicações como a barra de ferramentas da Google.

4.2.4.1 Requisitos

Para que esta funcionalidade seja implementada com sucesso, é necessária a criação de uma biblioteca em Java para acesso aos dados do Cartão de Cidadão através do wrapper disponível no Middleware do CC. Esta biblioteca terá depois de ser integrada numa applet que será enviada para o browser do utilizador no momento de acesso a uma página em concreto, que faça uso desta funcionalidade. Todos os conceitos associados a esta biblioteca estão definidos na secção 4.5 bem como os detalhes da sua estrutura.

Além desta camada intermédia de extrema importância em vários dos cenários discutidos ao longo da dissertação, importa também mencionar como requisito do caso de uso as implicações da sua utilização para os utilizadores. Tendo em conta que este mecanismo necessita de correr em Java no navegador, o utilizador terá de ter a compatibilidade com esta tecnologia instalada na sua máquina, o que apesar de uma coisa comum nos dias de hoje, pode ainda ser uma limitação em alguns computadores mais antigos ainda em uso.

4.2.4.2 Estrutura de Dados

Não existe necessariamente uma estrutura de dados obrigatória associada a este cenário, pelo menos na sua versão mais básica. A implementação desta solução passará pela criação de funções que, mediante parâmetros de entrada bem definidos, devolvam mecanismos para a obtenção dos dados desejados, não sendo necessário o armazenamento de nenhum tipo de configuração para isso. Por outro lado, uma ferramenta de detecção automática de campos de formulários com possível associação aos do CC necessitaria de uma solução de armazenamento de palavras e respectivas estruturas correspondentes no cartão, como a da figura 4.3.

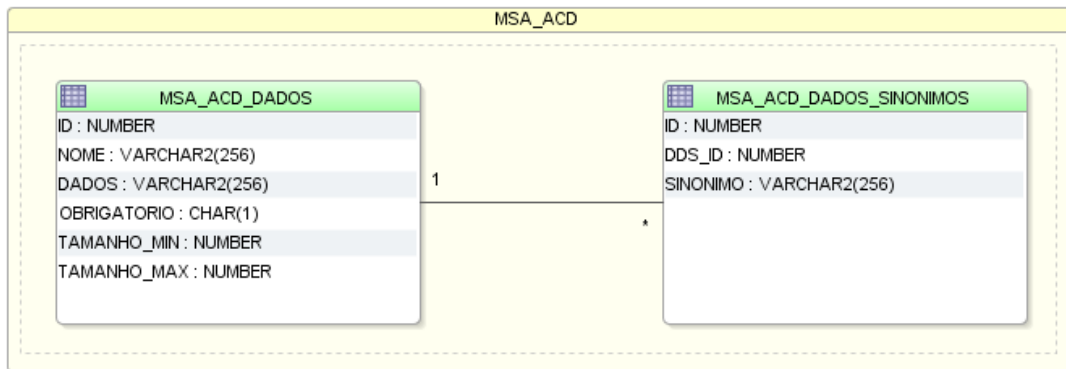


Figura 4.3: Estrutura de Dados para a detecção automática de dados do Cartão de Cidadão

No modelo apresentado acima, a tabela MSA_ACD_DADOS guarda a associação entre determinados nomes e dados do CC para simples consulta e ligação à lista de palavras que podem ser encontradas nos formulários com possível fonte no cartão, definida estruturalmente na tabela MSA_ACD_DADOS_SINONIMOS. É uma estrutura muito simples que serve apenas de base à implementação da funcionalidade. A complexidade mais uma vez está na criação de métodos para a pesquisa em tempo real num formulário por esse tipo de campos e consequente associação aos do CC.

4.2.4.3 Modo de Funcionamento

Do ponto de vista de utilização, o modo de funcionamento deste cenário é bastante simples sendo que, a complexidade está no lado da criação dos formulários que recorram a este método para a obtenção da informação armazenada no CC de cada utilizador. Quando o cidadão acede a uma formulário com dados associados ao cartão e este tiver sido configurado de maneira a poder fazer o pedido desses dados ao CC, em qualquer das abordagens discutidas acima sobre a apresentação da funcionalidade, deve ser dada ao utilizador a possibilidade de não usar este mecanismos e proceder à inserção manual dos dados. Da mesma forma, mesmo que os dados

tenham sido obtidos directamente do CC é boa prática apresentar ao utilizador um formulário de confirmação dos mesmos, com possibilidade de os alterar antes de submeter a informação.

4.2.5 Controlo de Acessos

Tendo em conta as desvantagens apresentadas na secção 3.2.1.5.4 e o tempo disponível para a implementação das restantes funcionalidades, não foi analisada para este cenário uma solução possível para o controlo de acessos integrado com o Cartão de Cidadão.

4.2.6 Controlo da Assiduidade

Tal como no cenário anterior, também no cenário do controlo da assiduidade com o Cartão de Cidadão as desvantagens apresentadas e sobretudo as restrições legais impostas pela CNPD na utilização do cartão para este tipo de funcionalidades, fizeram com que não fosse desenvolvida uma solução.

4.3 Assinatura Digital

O desenho de uma solução para a integração da assinatura digital com o Cartão de Cidadão nos contextos definidos nos cenários de utilização foi tudo menos simples. Além das aplicações externas e de alguns casos de empresas que dizem que implementaram uma solução integrada que permite a assinatura de algum tipo de documentos com o CC, não nos foi possível encontrar uma implementação baseada num SI para ultrapassar este problema.

Ambígua é provavelmente a palavra que melhor descreve a documentação analisada sobre o uso desta funcionalidade, a partir de uma estrutura Web. Em alguns momentos ficamos com a sensação que a assinatura pode ser efectuada directamente no cartão através do envio do bloco de caracteres a assinar, enquanto noutras situações está explicitamente definido que para assinar digitalmente com o CC é preciso obter o certificado de assinatura do cartão e fazer uso de funções externas para executar o algoritmo de assinatura sobre um conjunto de dados. De qualquer maneira, foram estudadas possibilidades com ambos os cenários e as conclusões a que chegámos estão definidas nesta secção.

4.3.1 Assinatura de Documentos

Hoje em dia, um número razoável de aplicações permite a inserção de assinaturas digitais num documento como é o caso do Microsoft Word, Adobe Acrobat e até o OpenOffice.org. Para este tipo de aplicações os limites são impostos pelos seus fabricantes e a compatibilidade com o CC é da sua inteira responsabilidade. O que nós temos de garantir da nossa parte é que em caso de inserção, a partir do SI, de uma assinatura digital, o documento tem de continuar a poder ser aberto na aplicação onde foi criado sem por em causa a sua integridade.

Por uma questão de limite temporal, definiu-se como prioridade apenas a implementação desta funcionalidade para documentos PDF. Assim, ficheiros PDF que sejam armazenados na base de dados, podem ser assinados digitalmente no momento da inserção no sistema. Para que isto seja possível não só seria necessário um método de assinatura no ou a partir do CC mas também serão precisos mecanismos internos para verificação dessas assinaturas. Outra questão

em aberto é a inclusão futura de documentos DOCX e ODT na lista de ficheiros passíveis de inclusão de assinatura a partir do SI.

4.3.1.1 Requisitos

É necessária a instalação de uma ferramenta como o iText na base de dados, que permite a inserção de assinaturas digitais em documentos PDF. A aplicação em si é bastante simples de usar e desde que lhe consigamos passar a chave privada de assinatura do cidadão, ela trata da execução do algoritmo respectivo. Neste caso concreto, deixa de ser necessário um mecanismo para assinatura de um conjunto de dados directamente no CC, o que minimiza em muito o tempo de implementação.

4.3.1.2 Estrutura de Dados

Não será necessária nenhuma estrutura de dados adicional para suportar este cenário de uso tendo em conta que cabe à aplicação de destino do ficheiro, normalmente o Adobe Reader, fazer a validação da assinatura. Talvez com a extensão da funcionalidade aos documentos DOCX e ODT venha a ser necessário um modelo de dados que suporte a sua utilização, mas até lá não há nada a acrescentar.

4.3.1.3 Modo de Funcionamento

Quanto à inclusão da assinatura digital do Cartão de Cidadão em documentos criados em aplicações externas, a AMA e os fabricantes possuem manuais bastante elucidativos das acções necessárias, pelo que não é da nossa competência a sua descrição.

Relativamente ao uso da assinatura interna ao SI de documentos PDF, o sistema deve ser capaz de, quanto um utilizador que tenha configurado a utilização do CC no SI, acede a um formulário com possibilidade de inserção de ficheiros, apresentar uma maneira de perguntar se deseja associar a sua assinatura ao documento. Depois do formulário submetido, caso o ficheiro seja PDF e o utilizador tenha escolhido a opção de adicionar assinatura o sistema deve solicitar o certificado digital do cidadão em questão, nomeadamente através de uma applet. O processo de verificação da assinatura na visualização dos documentos pertence à aplicação que efectua a leitura desse tipo de ficheiros.

4.3.2 Assinatura de Mensagens Electrónicas

Além das ferramentas de mail existentes, que implementam as funções de assinatura digital, não pode ser feito sobre os nossos servidores de mail para a inclusão automática de pedidos de certificados de assinatura dos cidadãos. Uma abordagem para este caso de uso pode ser a construção de uma pequena ferramenta que pode incluir duas funcionalidades distintas: a simples assinatura de um determinado texto que pode ser copiado pelo utilizador e usado onde este o entender ou então um método básico de envio de mensagens electrónicas dentro do próprio SI, onde o utilizador define os destinatários, assunto e corpo da mensagem a enviar, sendo que no momento de envio o sistema envia um pedido do certificado do CC através de uma applet.

4.3.2.1 Requisitos

Para a implementação das ferramentas descritas acima, os requisitos são os mesmos que os definidos na solução do cenário de Assinatura de Documentos e estão apenas relacionados com o acesso à assinatura digital contida no Cartão de Cidadão.

4.3.2.2 Estrutura de Dados

Por uma questão de simplificação de implementação e tendo em conta que não estamos a desenvolver um sistema de envio de mensagens electrónicas, mas sim uma funcionalidade extra ao SI para a utilização desse serviço, não será necessária uma estrutura de dados que suporte a gestão das mensagens enviadas pelos utilizadores. Assim, não há nada a acrescentar ao modelo com a inclusão das operações descritas acima.

4.3.2.3 Modo de Funcionamento

O modo de funcionamento da funcionalidade é bastante simples e o acesso às ferramentas deve ser feito através de uma área criada para o efeito, sendo que este acesso só deve ser permitido aos utilizadores que tenham configurada a utilização do CC no SI. No caso de uso mais simples, o utilizador introduz simplesmente o texto que quer assinar e o sistema gera o conteúdo da assinatura que deve ser anexo à mensagem na ferramenta de mail. Na ferramenta de envio de mensagens, além do corpo da mensagem, o utilizador deve também definir os destinatários e o assunto da mesma, e no momento de envio o sistema envia um pedido ao CC pelo certificado de assinatura. O resultado da aplicação do algoritmo ao conteúdo é anexo ao corpo da mesma e o sistema encarrega-se de enviar o mail para os destinatários especificados.

4.3.3 Assinatura de Conteúdos da Base de Dados

Ambicioso, mas extremamente complexo. Esta é melhor definição do cenário de utilização da assinatura digital do Cartão de Cidadão no armazenamento de informação assinada na base de dados. As alternativas analisadas para o armazenamento deste tipo de informação foram muitas, desde abordagens à utilização de XML específico para assinaturas digitais (XMLDsig), passando pela extensão do tamanho máximo permitido para o limite máximo da tecnologia da base de dados de todas as colunas onde se pode vir a armazenar informação concatenada com a assinatura, até à criação de colunas auxiliares nas tabelas em questão.

Todas as soluções discutidas até agora têm vantagens e desvantagens mas nenhuma delas garante a flexibilidade desejada ao SI. Se tivermos em consideração as colunas das tabelas em que o tamanho máximo permitido é também o permitido pela Oracle, a anexação da assinatura ao conteúdo do campo limitaria o seu tamanho máximo, o que nem sempre é possível. Outra questão não resolvida por nenhum dos mecanismos analisados até agora, é a maneira como seria feita a verificação de que se um campo em concreto tinha sido assinado ou não, isto é, como é que num campo de preenchimento livre se pode ter a certeza se está presente ou não a assinatura associada? E se, apesar do esforço necessário ou das limitações impostas por estes mecanismos, é possível fazer com que de alguma maneira estes funcionem para a assinatura de um campo ou campos de uma tabela em concreto, nenhum apresenta uma solução para a assinatura conjunta de múltiplos registos de múltiplas tabelas da base de dados.

A garantia da implementação de uma solução que cubra todos os pontos descritos passa por uma estrutura altamente flexível de armazenamento de dados digitalmente assinados. Este

tipo de estrutura pode-se revelar ligeiramente mais lento que os outros no ponto de vista de acesso aos dados mas as vantagens que introduz a todos os níveis quase que anulam esse factor. É então neste contexto que é apresentada uma solução para a inclusão de assinaturas digitais no SI.

4.3.3.1 Requisitos

Não há nenhum requisito a acrescentar aos que foram listados para a utilização do CC como método de assinatura digital nas secções 4.3.1 e 4.3.2, à excepção de que as tabelas onde a assinatura digital vai ser instalada não podem ser tabelas particionadas ou tabelas organizadas por índice dinâmico.

4.3.3.2 Estrutura de Dados

Para armazenar a assinatura de conteúdos da base de dados sobre uma estrutura existente, a melhor solução encontrada foi uma divisão do modelo de suporte à funcionalidade em duas componentes distintas: um modelo mais simples que cobre o caso mais simples da assinatura de um campo, de um registo e de uma tabela em concreto, e outro que cobre o cenário da assinatura de múltiplos registos de uma ou mais tabelas. Existem bastantes semelhanças entre os dois, principalmente na maneira como a chave simétrica encriptada e a cifra do conteúdo assinado são armazenados, sendo que a diferença reside na lógica da estrutura de captura de valores a validar.

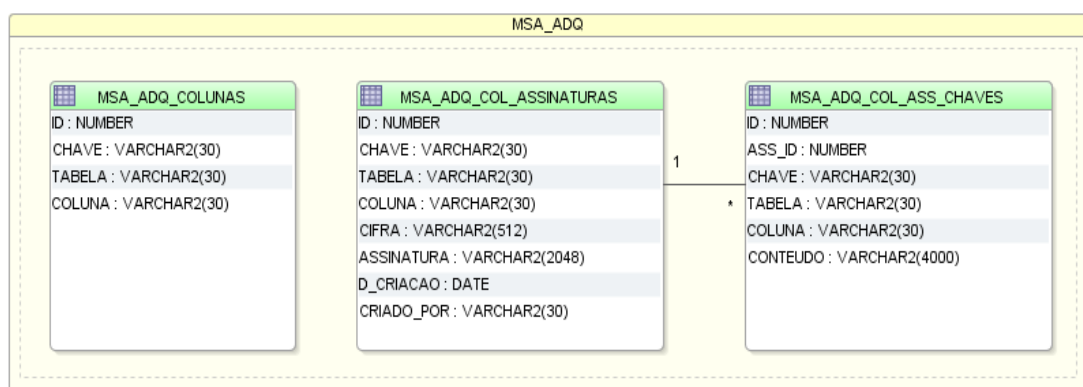


Figura 4.4: Estrutura de Dados para a Assinatura de Colunas na Base de Dados

O modelo apresentado na figura 4.4 está relacionado com a funcionalidade da assinatura de colunas específicas da base de dados e está por sua vez dividido em duas áreas: uma para a gestão das colunas que podem ser assinadas e outra para a gestão das assinaturas associadas. A tabela MSA_ADQ_COLUNAS armazena informação sobre a coluna de uma tabela e a respectiva chave primária que pode ou não ser assinada pelo utilizador e considerando, por exemplo, uma coluna chamada CONTEUDO da tabela MENSAGENS, essa informação deve ser armazenada na tabela em causa. A tabela, MSA_ADQ_COL_ASSINATURAS, inclui mais uma vez os nomes da coluna, tabela e chave primária da tabela de destino da assinatura. O resto das colunas desta tabela estão associadas à gestão da assinatura propriamente dita e são exactamente iguais aos descritos nas secções anteriores. A localização única dos registos assinados digitalmente é garantida pela tabela MSA_ADQ_COL_ASS_CHAVES, que através do armazenamento de um

Solução Proposta

conjunto de informações único a um determinado registo, permite a sua posterior identificação única na base de dados em causa. Através do conjunto TABELA, COLUNA e CONTEUDO, o sistema consegue chegar aos registos em causa.

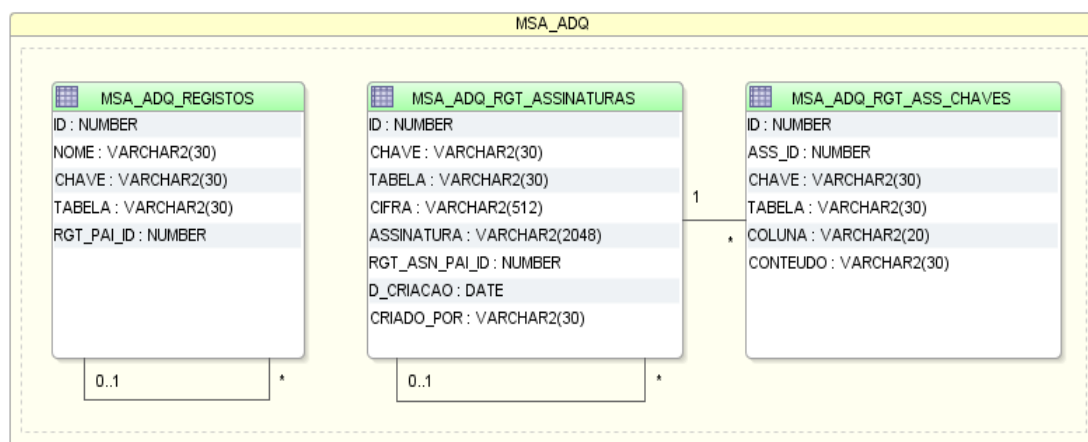


Figura 4.5: Estrutura de Dados para a Assinatura de Registos na Base de Dados

À semelhança do modelo anterior, o da figura 4.5 apresenta uma possível estrutura para a implementação da assinatura digital de registos da base de dados. Tal como na solução, também esta supõe uma área de configurações onde um administrador define quais as tabelas que podem ter os seus registos assinados, os filhos associados e um nome de referência. Essa gestão é feita através da tabela MSA_ADQ_REGISTOS. O armazenamento das assinaturas e a ligação aos registos por elas assinados é feito na tabela MSA_ADQ_RGT_ASSINATURAS, onde a única excepção para o modelo anterior é a possível ligação a um registo pai. A localização única dos registos é feita através da tabela MSA_ADQ_RGT_ASS_CHAVES.

4.3.3.3 Modo de Funcionamento

Ao contrário de todas as soluções apresentadas até agora, esta é a única que necessita de intervenções em áreas distintas: pelos administradores no sentido de configurarem as colunas ou tabelas que podem receber assinaturas, pelos programadores que têm de rever o código de maneira a incluir chamadas a uma API a desenvolver e pelos utilizadores no sentido de efectuar a assinatura dos conteúdos da base de dados. No que diz respeito à administração do sistema em causa, as funcionalidades a implementar serão simples páginas de configuração das tabelas e colunas que podem ser assinadas digitalmente com o CC. A nível de adaptação da estrutura de código existente para a inclusão da validação da assinatura posteriormente inserida ou não, será necessária a chamada a funções do MSA que primeiro verificam se está definida, para uma dada coluna ou tabela, a possibilidade de assinatura digital associada e, em caso afirmativo, se existe realmente uma assinatura válida ligada a esse campo ou registo.

Do ponto de vista da utilização e da integração com o Cartão de Cidadão, em cada página onde seja permitida a assinatura digital qualificada com o certificado correspondente, deve ser permitido ao utilizador seleccionar uma opção de inserção ou não da sua assinatura, a não ser que esta seja obrigatória para esse caso em concreto. Nas páginas de visualização de conteúdos possivelmente assinados, devem estar definidos métodos capazes de gerar informação associada à validade da assinatura inserida ou não, isto é, se por exemplo um aluno aceder à página com

as classificações de uma disciplina, deve existir uma secção nessa página que confirme que esses registos foram efectivamente criados pelo responsável da disciplina em questão.

4.4 Encriptação

A utilização da encriptação através do Cartão de Cidadão supõe sempre o recurso a uma estrutura à parte para efectuar a gestão de chaves simétricas a serem utilizadas na encriptação e desencriptação de dados no SI, tendo em conta que não foi disponibilizada nenhuma estrutura do género integrada no CC. Este problema tem tanto de complexo como de inovador e a utilização desta componente depende muito do sucesso que venha a ser alcançado com a implementação da estrutura associada aos mecanismos necessários para a encriptação.

De uma forma geral, e porque não existe nenhuma chave no CC para encriptação de dados, a estrutura a ser implementada tem de assegurar a troca de chaves de forma segura entre os utilizadores da instituição. Estas chaves devem ser encriptadas utilizando por exemplo a chave pública de assinatura digital associada ao cidadão, isto é, se eu quiser enviar um conjunto de dados de forma encriptada para outro utilizador o SI deve ser capaz de, depois de identificado o destinatário dessa informação, gerar uma chave simétrica aleatória e ir buscar a chave pública de assinatura digital do utilizador para proceder à encriptação da chave simétrica. Os dados encriptados, juntamente com a chave simétrica encriptada, são enviados para o destinatário que, através da sua chave privada de assinatura digital consegue desencriptar a chave simétrica e a partir dessa consegue também proceder à desencriptação dos dados.

4.4.1 Encriptação de Documentos

Numa fase inicial, a encriptação de documentos será sempre feita pelas aplicações a que cada um pertence através de utilização da funcionalidade, disponível em quase todas as ferramentas, da poder guardar um documento encriptado com uma palavra-passe. Do ponto de vista de integração com a solução de encriptação disponibilizada pelo SI, esta palavra-passe a utilizar nas ferramentas respectivas é a chave simétrica gerada aleatoriamente pelo sistema, que depois de usada para a encriptação do documento deve ser enviada ao destinatário de forma encriptada com o recurso à chave pública de assinatura digital desse destinatário, juntamente com o documento encriptado.

A maneira como o envio do documento e da respectiva chave assimétrica encriptada é feito fica a cargo do utilizador, mas para que exista uma alternativa interna ao SI, deverá ser criada uma área de gestão de documentos encriptados com o Cartão de Cidadão de tal forma que em vez de enviar o documento e a chave, por exemplo, por mail, a gestão desses documentos pode ser feita internamente no SI. Esses documentos podem ficar armazenados temporariamente na base de dados, sendo automaticamente removidos no final do prazo.

4.4.1.1 Requisitos

Além do requisito óbvio que é a estrutura de encriptação a funcionar, este cenário supõe também que o remetente sabe à partida quem são os destinatários do documento e quais as chaves públicas de cada um deles e onde podem ser alcançadas. Mas o maior problema desta implementação está ligado com o facto de ser necessário gerar uma versão encriptada da chave simétrica para cada destinatário do documento, o que se considerarmos um grupo de utilizadores com por exemplo 100 pessoas, origina o mesmo número de registos de chaves

encriptadas. Numa utilização em larga escala a gestão deste mecanismo pode se tornar pesada mas como as chaves são apenas armazenadas por um período de tempo pré-definido, pode ser considerado um problema com pouco impacto na implementação final.

Importa também mencionar mais uma vez como requisito a necessidade da existência da camada de acesso ao certificado digital de assinatura do CC. Sem esta funcionalidade, não é possível aceder à chave privada do destinatário no momento da descriptação da chave para descriptação do conteúdo do documento, o que torna este caso de uso desnecessário.

4.4.1.2 Estrutura de Dados

A estrutura de dados para suporte à encriptação de documentos não é complexa. Para uma versão básica da funcionalidade basta suportar o armazenamento de documentos de uma forma genérica e uma lista de destinatários com as chaves simétricas dos documentos encriptados com a chave pública de assinatura digital de cada um. O modelo da figura 4.6 ilustra o contexto aqui descrito.

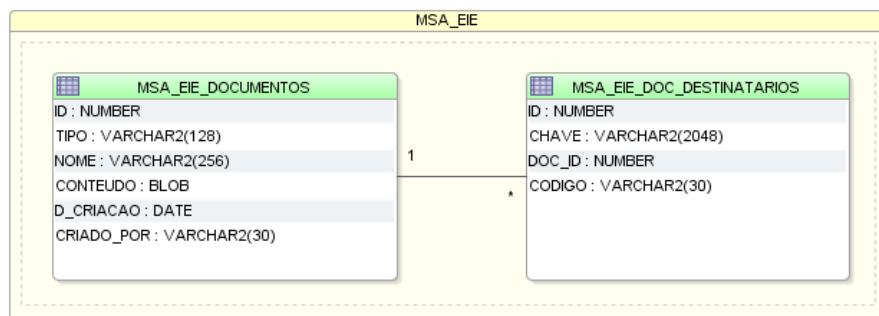


Figura 4.6: Estrutura de Dados para a Encriptação de Documentos

Como podemos confirmar depois de observarmos o modelo em questão, os documentos são armazenados na tabela MSA_EIE_DOCUMENTOS depois de encriptados e os utilizadores que têm acesso ao mesmo são guardados na tabela MSA_EIE_DOC_DESTINATARIOS.

4.4.1.3 Modo de Funcionamento

Admitindo que todos os pressupostos envolvidos na criação da estrutura de suporte ao caso de uso são implementados com sucesso, a funcionalidade deve ser utilizada de molde a permitir ao utilizador que deseja proceder à encriptação de um documento a possibilidade de escolha entre se quer apenas usar o mecanismo de geração aleatória de chaves simétricas e enviar o conjunto isoladamente, ou se também deseja usar o sistema de armazenamento de documentos do SI.

Em qualquer dos cenários, o primeiro passo para o funcionamento deste caso de uso é o pedido de uma chave simétrica aleatória. Após esse pedido, o utilizador deve proceder à encriptação do documento na ferramenta respectiva. Mesmo que opte por não usar o sistema de armazenamento de documentos, o utilizador tem na mesma de seleccionar os destinatários do documento e no seguimento dessa acção, estes serão notificados com uma mensagem para acederem ao SI e descriptar a chave de acesso ao documento.

4.4.2 Encriptação de Mensagens Electrónicas

A solução para a implementação deste cenário é muito semelhante à descrita na secção anterior para a encriptação de documentos, sendo que em vez de um sistema de armazenamento de ficheiros, a base de dados necessita de ser equipada com um mecanismo que permita o alojamento de mensagens e permissões para os respectivos destinatários. Também como no caso de uso anterior, a encriptação de mensagens electrónicas pode ser feita com ferramentas de mail externas, sendo o SI responsável apenas pela geração aleatória de chaves simétricas.

4.4.2.1 Requisitos

Não há nada de novo a acrescentar aos requisitos definidos na secção 4.4.1 para o cenário de Encriptação de Documentos pela semelhança de funcionalidades a implementar entre ambos.

4.4.2.2 Estrutura de Dados

Se o modelo de dados necessário para o cenário anterior de encriptação de documentos não era complexo, então a estrutura de dados necessária para este cenário é ainda menos. É bastante semelhante ao apresentado na solução do cenário anterior e os principais conceitos estão relacionados com o armazenamento dos destinatários e as respectivas versões encriptadas da chave simétrica para desencriptação do conteúdo da mensagem. A figura 4.7 mostra o modelo de dados de suporte ao cenário de encriptação de mensagens electrónicas.

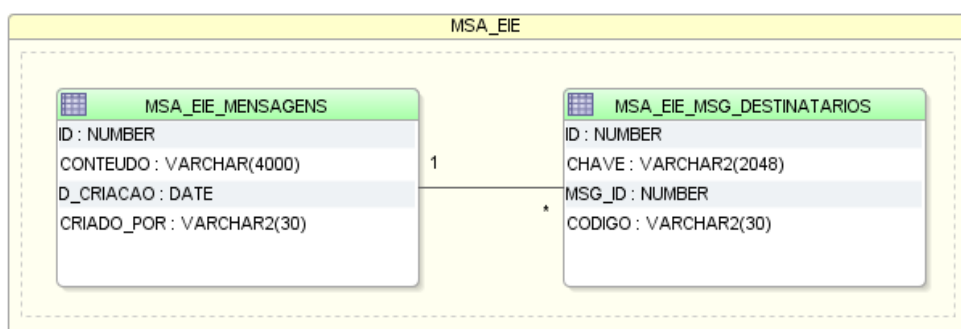


Figura 4.7: Estrutura de Dados para a Encriptação de Mensagens Electrónicas

À semelhança do modelo do cenário anterior, o sistema deve permitir, neste caso concreto, o armazenamento de mensagens enviadas, através da tabela MSA_EIE_MENSAGENS, por um período limitado de tempo, as quais deverão ser disponibilizadas aos destinatários da mensagem que possuam a chave privada capaz de efectuar o processo de desencriptação da chave com sucesso. Esta informação fica guardada na tabela MSG_EIE_MSG_DESTINATARIOS.

4.4.2.3 Modo de Funcionamento

Para a implementação desta funcionalidade é necessário um esquema semelhante ao que foi introduzido no cenário de Encriptação de Documentos, isto é, para o de envio de mensagens com ferramentas externas, o utilizador deve simplesmente aceder a uma página do SI dedicada para o efeito, e depois de introduzir o corpo da mensagem e seleccionar os destinatários que

pretende, o sistema deve gerar o conteúdo encriptado do texto a ser copiado para a ferramenta e automaticamente enviar uma notificação para os destinatários com uma ligação onde podem visualizar a chave simétrica encriptada e proceder à sua desencriptação.

Da mesma forma, a implementação de uma funcionalidade mais complexa dentro deste cenário passa pelo mesmo processo inicial de introdução do corpo da mensagem e selecção dos destinatários, a juntar à descrição do assunto. De seguida, e ao contrário da abordagem anterior, o SI envia a mensagem electrónica encriptada aos destinatários, juntamente com a ligação para a página onde podem efectuar a desencriptação da chave.

4.4.3 Encriptação de Conteúdos da Base de Dados

Alvo de muitas discussões, não só nesta dissertação mas também em muitos documentos científicos, o cenário de encriptação de conteúdos da base de dados é sempre um caso sensível, que merece a atenção de todas as partes envolvidas no armazenamento da informação. Não só é muito importante para o utilizador poder ter a confiança que os dados sensíveis que registou no SI não estão ao alcance pelo menos de todos os funcionários responsáveis pela administração da base de dados, mas também é importante para a instituição a utilização de um sistema de envio de informação de forma segura, quase impossível de desencriptar, se a comunicação for interceptada.

Se o mecanismo de Encriptação Transparente de Dados, disponibilizado pela Oracle no seu módulo de Segurança Avançada, permite a mudança de paradigma estrutural de uma forma quase transparente, tal como o próprio nome indica, qualquer outro mecanismo que implemente funcionalidades semelhantes vai sempre implicar um trabalho de adaptação consideravelmente elevado. A solução da Oracle tem imensas vantagens mas não é perfeita, a começar pelo custo financeiro de aquisição do seu módulo de segurança avançado e a terminar na gestão central de chaves simétricas. De uma forma não muito complexa e com relativamente pouco detalhes vamos apresentar uma solução para a abordagem a este problema com a utilização do Cartão de Cidadão como base de referência e a estrutura intermédia de encriptação como suporte.

Acima de tudo, e tal como foi estabelecido para a implementação de cenário de Assinatura de Conteúdos da Base de Dados, o mais importante é que a estrutura em causa garanta a maior flexibilidade possível e minimize o número de alterações a introduzir no sistema existente de maneira a suportar esta funcionalidade. Assim, ao longo desta secção, serão descritas as medidas e pressupostos a ter em conta e a direcção a tomar no desenvolvimento de uma solução.

4.4.3.1 Requisitos

Tirando os requisitos associados ao uso do certificado de assinatura digital do CC através do SI, não existem graves limitações da solução a implementar. Há, no entanto, pormenores que é necessário ter em conta, como é o caso das restrições associadas ao tipo de tamanho dos dados que podem ser encriptados e, de seguida, armazenados na base de dados. Numa primeira análise a esta questão não deve haver muitas limitações dos campos, à excepção dos do tipo LOB, que podem vir a originar alguns conflitos com os algoritmos de encriptação.

4.4.3.2 Estrutura de Dados

A estrutura necessária para suportar os mecanismos de encriptação descritos ao longo da dissertação é semelhante, no lado da administração, àquela que foi apresentada para a assinatura

de colunas da base de dados, na secção 4.3.3.2. Também aqui será necessária uma área de administração para definir quais são as colunas e de que tabelas são, que devem ou podem ter o seu conteúdo encriptado. O restante modelo está mais ligado à utilização das funcionalidades em concreto e à maneira como as chaves simétricas encriptadas são atribuídas aos utilizadores, em função dos certificados digitais de assinatura respectivos. A figura 4.8 inicia a discussão da estrutura adoptada neste cenário.

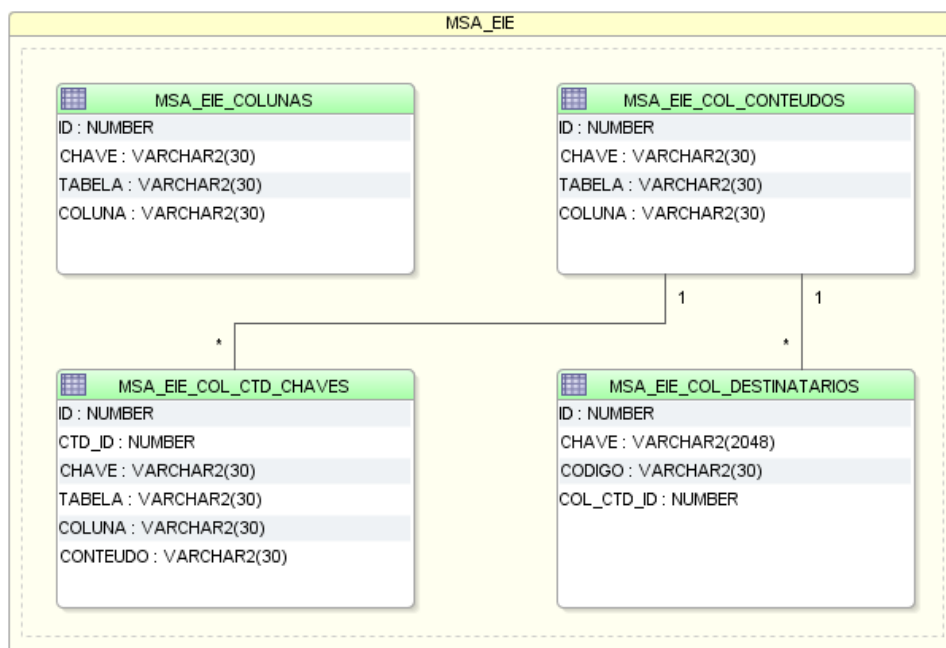


Figura 4.8: Estrutura de Dados para a Encriptação de Conteúdos da Base de Dados

Depois de observar o modelo é possível perceber que a tabela MSA_EIE_COLUNAS é o local onde serão armazenadas as configurações associadas à lista de colunas que podem ser encriptadas no SI. Esta tabela está completamente isolada do resto da estrutura e serve apenas como referência ao MSA e às utilizações que o utilizem através da API. Toda a gestão dos dados encriptados e das chaves de desencriptação necessárias é mantida em paralelo através das tabelas MSA_EIE_COL_CONTEUDOS e MSA_EIE_COL_DESTINATARIOS, enquanto que a localização única dos registos é feita através da tabela MSA_EIE_COL_CTD_CHAVES. Enquanto que a primeira tabela serve para nos indicar quais são os campos dos registos que estão efectivamente encriptados, a segunda tem por base o armazenamento das chaves simétricas encriptadas que os destinatários serão capazes de desencriptar. A ligação múltipla entre as duas tabelas tem a ver com o facto de, para o mesmo conteúdo, poderem existir diversos destinatários que o utilizador ache que devem ser capazes de ter acesso à informação guardada na base de dados de forma encriptada. A última funciona da mesma forma que a localização única de registos na base de dados, como apresentado na secção das assinaturas digitais.

4.4.3.3 Modo de Funcionamento

A administração desta funcionalidade é idêntica à da gestão das configurações para as colunas e tabelas que pode ser assinadas digitalmente, tal como é mencionado na secção 4.3.3.3,

onde os administradores do SI podem também aqui proceder à modelação das colunas que podem ter o seu conteúdo encriptado. E mais uma vez, tal como na secção referida atrás, o código das páginas que insere ou mostra conteúdo de colunas que estão configuradas para o registo de dados encriptados, terá de ser alterado de maneira a executar as devidas chamadas de descriptação, se a informação estiver efectivamente encriptada.

No que diz respeito à utilização das funcionalidades de encriptação de dados no SI, os utilizadores devem ter a possibilidade de optar pela encriptação ou não dos conteúdos a inserir ou alterar no sistema, assim como devem poder escolher a lista de destinatários com acesso às funções de descriptação e posterior visualização dos dados guardados na base de dados, sendo que por defeito o utilizador que efectua a encriptação é ele próprio adicionado automaticamente aos destinatários da descriptação. Quando um utilizador entra numa página com conteúdo encriptado por ele próprio ou por outros utilizadores, o SI deverá executar os mecanismos de descriptação e, em caso de sucesso, disponibilizar essa informação ao utilizador em questão.

4.5 Biblioteca de Software para o Cartão de Cidadão

Portuguese eID for Java (PTEID4J), é o nome da biblioteca em Java a implementar para a integração da utilização do Cartão de Cidadão com o SI. É uma biblioteca em código aberto que deve ser disponibilizada à comunidade e foi nomeada em inglês de maneira a estender a sua utilização a entidades estrangeiras que queiram desenvolver aplicações que interajam com o CC português. Funciona como uma camada intermédia entre código aplicacional, no nosso caso em concreto PL/SQL, e as funções de acesso ao CC disponibilizadas pela biblioteca PTEIDLIB que é automaticamente instalada com o Middleware do Cartão de Cidadão.

O código de geração das applets de acesso aos certificado do CC, várias vezes mencionado no decorrer deste capítulo, deve também ser inserido neste pacote de procedimentos Java. É também importante que estejam disponíveis nesta interface mecanismos alternativos. Por exemplo, no caso da assinatura digital, devem ser implementadas funções que retornem não só o certificado digital associado à assinatura mas também métodos de assinatura directa no cartão com o uso das técnicas do PKCS#11. Apesar de a nossa decisão passar por deixar a autenticação de utilizadores a cargo do Apache, é também interessante implementar mecanismos de acesso através da PTEID4J.

A biblioteca teve como fonte de inspiração o projecto eid-applet, uma biblioteca para o uso do Cartão de Cidadão belga que é em muitos aspectos semelhante ao existente em Portugal, disponível no Google Code, também em código aberto. Existem também abordagens deste tipo de implementações para o CC da Áustria e da Estónia mas não tão completas como o exemplo da Bélgica.

4.6 Arquitectura

Ao longo deste capítulo foram sendo apresentados partes das componentes que compõem aquela que é a arquitectura associada ao projecto. Nesta secção é feita uma descrição global das diversas áreas de intervenção e da maneira como a comunicação entre estas componentes será feita no SI. Pretende-se que a solução seja o mais independente e flexível possível mas não podemos ignorar como é óbvio o ambiente que a rodeia, com potencialidades e limitações em todos os aspectos.

4.6.1 Divisão Funcional

Para que o conjunto de soluções a implementar fique completamente isolado do sistema actual decidimos criar um módulo independente, o Módulo de Segurança Avançado (MSA), que pode ser instalado ou removido da aplicação com muito pouco esforço de implementação dos outros módulos que a constituem. No caso concreto do agrupamento GESSI / SIGARRA e tendo em conta que se tratam de um módulo avançado de gestão de informação será melhor transportar estas funcionalidades para aquele que é o motor do SI, o GESSI. E porque dentro deste módulo estão envolvidas diversas componentes distintas, é sugerida uma divisão interna do módulo tal como é ilustrada na figura 4.9.

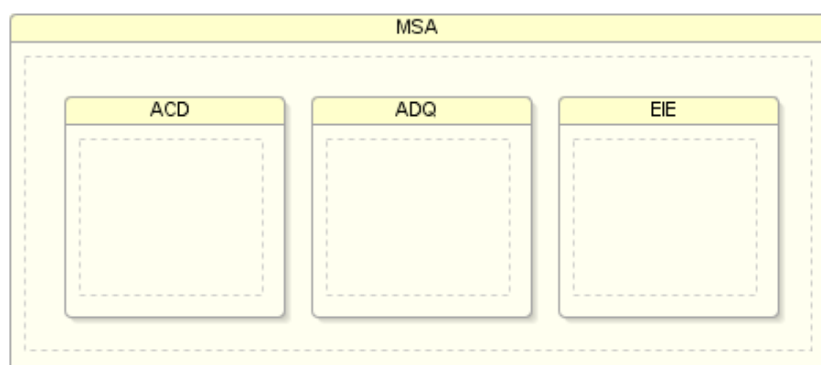


Figura 4.9: Divisão Funcional da Arquitectura da Solução Proposta

Como podemos observar então o MSA está dividido em três grandes áreas de acordo com a divisão dos cenários de utilização apresentados no capítulo 3. Assim temos para a componente de Autenticação o módulo de Autenticação com Certificados Digitais (ACD), para a Assinatura Digital o módulo de Assinatura Digital Qualificada (ADQ) e para a Encriptação o módulo de Estrutura Intermédia de Encriptação (EIE). Nesta divisão foram apenas analisadas componentes da base de dados com área de intervenção associada, não tendo em conta outras componentes como a API a disponibilizar para integração com as aplicações existentes e a camada de ligação com o PTEID4J para interacção com o CC.

4.6.2 Lógica de Negócio

Depois de apresentada a divisão funcional do módulo que se presente desenvolver, é ainda importante perceber qual a lógica de negócio associada à implementação deste grupo de funções e que cuidados devem ser tidos em consideração. Acima de tudo é de esperar que cada área do módulo seja independente o mais possível das outras componentes, principalmente se estiverem em camadas diferentes da estrutura do sistema. A figura 4.10 mostra as camadas pensadas para a implementação da aplicação e o fluxo de informação entre elas.

Solução Proposta

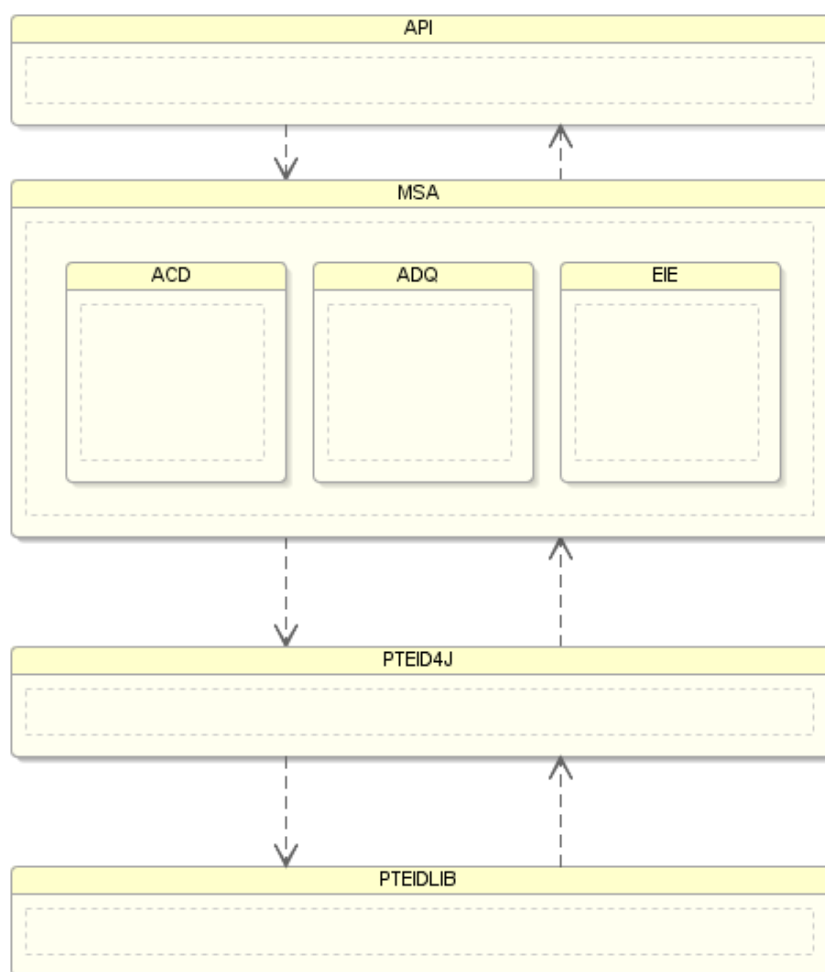


Figura 4.10: Lógica de Negócio da Arquitectura da Solução Proposta

Como é simples de perceber o cérebro da arquitectura proposta que está no MSA e nos diversos módulos que o constituem, sendo que a integração com outras aplicações ou com outros módulos dentro do GESSI só deverá ser feita através da camada acima, a API. Ambas as camadas do MSA e da API estão localizadas na base de dados e a sua implementação será feita com PL/SQL. A componente PTEID4J apesar de também estar armazenada na base de dados, é uma biblioteca Java que disponibiliza uma interação com a biblioteca do Middleware do Cartão de Cidadão, a PTEIDLIB, estando esta última instalada no computador de cada utilizador que acede às funcionalidades do módulo.

4.7 Resumo

Ao longo deste capítulo foram discutidas soluções de implementação das funcionalidades apresentadas no capítulo anterior. Como estava mais ou menos previsto, devido à panóplia de tecnologias e conceitos abrangidos, a complexidade associada a algumas destas implementações é considerável, o que pode pôr em causa a sua conclusão naquele que é o tempo previsto para desenvolvimento e apresentação de resultados. Assim, ao longo da implementação, e consoante

Solução Proposta

as barreiras encontradas no caminho, vão ser definidas metas reais de desenvolvimento, isto é, quais são as componentes que podem efectivamente ser implementadas e integradas o mais possível com o SI.

No que diz respeito à arquitectura e modelos das soluções propostas, é de salientar uma divisão por camadas que

5 Implementação

Neste capítulo são apresentados os desenvolvidos efectuados, as configurações necessárias e as metodologias adoptadas no decorrer da implementação do projecto. Serão também feitas referências aos mais diversos problemas encontrados no decorrer da dissertação e as soluções para a sua correcção ou as justificações para a sua impossibilidade. São ainda descritas as normas de implementação das instituições a maneira como o código das diversas componentes está organizado.

5.1 Introdução

Devido à complexidade e dimensão das funcionalidades abordadas ao longo da dissertação, a maior parte do tempo foi alocado à pesquisa de cenários e soluções para a utilização do Cartão de Cidadão como meio de autenticação, transmissor de integridade e consistência de dados ao SI. Assim, as implementações desenvolvidas durante o projecto concentram-se mais na viabilidade das soluções apresentadas e na maneira como será feita, na realidade, a integração de todas as componentes num único sistema.

Foram desenvolvidos no decorrer da implementação diversos testes que visam a validação de tudo aquilo que foi apresentado em teoria, tanto a nível de custo de implementação como a nível de limitações logísticas e tecnológicas existentes. Estes testes permitem ter uma noção muito próxima da realidade, de como vai funcionar o sistema analisado, e servem também para introduzir aquilo a que normalmente se chama de prova de conceito da dissertação.

5.2 Nomenclaturas

Relativamente à nomeação de objectos e procedimentos, a equipa de desenvolvimento da instituição tem regras bem especificadas que devem ser seguidas, de maneira a estabelecer uma linha de desenvolvimento único, para posteriores análises de código mais eficientes. Quando à definição dos módulos, é boa prática escolher também acrónimos de 3 ou 4 letras associadas ao nome desse módulo, que possam vir a ser usados ao longo do desenvolvimento da aplicação.

5.2.1 Java

Ao nível de código Java, não sendo esta a plataforma de desenvolvimento principal da equipa, não existem regulamentos internos quanto à nomeação de classes e variáveis a usar. No entanto, e tendo em consideração a linguagem de programação em si, foram sempre seguidas regras associadas à tecnologia, como por exemplo a nomeação de classes sem espaços e com letras maiúsculas no início de cada palavra que constituem esse nome, e a definição de variáveis com uma letra minúscula no início do nome, mas nas restantes que o constituem foi utilizada a mesma nomenclatura das classes.

5.2.2 PL/SQL

Sendo que esta é linguagem mais usada na instituição, existem diversas regras associadas à criação de pacotes, tabelas, funções e procedimentos para uma melhor uniformização do código desenvolvido para a instituição. Entre prefixos e sufixos, é importante lembrar que, devido à limitação imposta na base de dados, em que o tamanho máximo do nome dos objectos não pode ultrapassar os 30 caracteres. Esta limitação implica por vezes o uso de demasiados acrónimos e dificulta o processo de análise de situação. Voltando ainda à questão do nome dos módulos, todos os objectos associados de alguma forma a um determinado módulo devem ter o seu nome anexado ao acrónimo do módulo.

Tabela 5.1: Sufixos dos Pacotes em PL/SQL

<i>Sufixo</i>	<i>Descrição</i>
_API	Pacote da Camada Intermédia de Funções de Acesso a um Módulo
_BR	Pacote da Lógica de Negócio
_BRA	Pacote da Lógica de Negócio (gerado automaticamente)
_C	Pacote de Cursores
_CA	Pacote de Cursores (gerado automaticamente)
_DM	Pacote de Acesso a Dados
_DMA	Pacote de Acesso a Dados (gerado automaticamente)
_GERAL	Pacote Geral
_INT	Pacote de Visualizações
_INTA	Pacote de Visualizações (gerado automaticamente)
_TP	Pacote de Tipos de Dados
_TPA	Pacote de Tipos de Dados (gerado automaticamente)
_VLD	Pacote de Validação
_VLDA	Pacote de Validação (gerado automaticamente)

A tabela 5.1 mostra uma lista de sufixos actualmente em actualização para o nomeação de pacotes pela equipa de desenvolvimento da instituição. Como podemos observar, existem vários pacotes gerados automaticamente através de uma ferramenta interna, o Gerador de Código, que consoante um conjunto de tabelas de um módulo especificado, gera uma camada de funções e

procedimentos para acesso a dados, visualizações e validações de dados associadas. Todos os pacotes criados no MSA seguiram as normas impostas pela instituição.

5.3 MSA

Toda a implementação do Módulo de Segurança Avançada foi e deve continuar a ser feita de maneira a que as ligações entre as diferentes componentes seja transparente entre cada uma delas e entre módulos ou aplicações externas, isto é, uma determinada componente ou módulo externo não precisam de saber de como é que a estrutura de uma funcionalidade foi criada, mas apenas quais são as suas funções de API e como devem ser chamadas. Também a ter em conta nesta fase é que mesmo dentro de cada componente, deve existir uma forte independência nas diversas camadas da aplicação que utilizam pacotes distintos, com um número de dependências muito pequeno ou quase nulo, tal como estão listados na tabela 5.1.

5.4 PTEID4J

A biblioteca Java de acesso ao Cartão de Cidadão deve ter um arquitectura de classes bem definida, organizada em pacotes distintos consoante a sua utilidade final. Esta estrutura deve permitir ao programador, no caso de querer apenas as funcionalidades mais básicas do sistema, não necessitar de incluir todos estes pacotes no seu projecto. O armazenamento do projecto, como foi dito anteriormente, está no Google Code, ferramenta que disponibiliza um leque de opções muito interessante para desenvolvimento de código aberto, como, por exemplo, uma capacidade de versionamento muito estruturada.

De maneira a que a applet do PTEID4J venha a submeter parâmetros para as páginas que implementarem a solução, é necessária a utilização da DOM da respectiva página, o que pode vir a ser um problema, nas situações em que temos de esperar por ele.

5.5 Autenticação

Desde o início do projecto, esta foi a área à qual foi dedica mais atenção, tendo em conta que esta era a funcionalidade mais prioritária que se queria implementar no SI, e que sem o sucesso desta, os outros mecanismos dificilmente seriam possíveis de implementar. O caminho que seguimos para a sua implementação, numa primeira fase, foi o uso do Apache para efectuar o pedido dos certificados de autenticação ao Cartão de Cidadão, tal como foi mencionado na secção 4.2.1. Ao longo desta secção são apresentados passos necessários para a utilização desta funcionalidade no SI.

5.5.1 Configurações

Depois de muito trabalho escondido e ao fim de alguns dias de investigação, finalmente conseguimos que o Apache efectuasse pedidos ao leitor do CC. Trabalho escondido porque é muito complicado medir o grau de progresso de uma coisa que não se pode mostrar, como é o caso aqui na definição das configurações do Apache. Foi especialmente nesta componente da implementação que constatamos a falta de informação disponível para a configuração de outros

Implementação

servidores web que não o IIS da Microsoft, nem mesmo da parte das entidades competentes. A figura 5.1 reflecte o trabalho de vários dias de pesquisa e testes para possíveis integrações.

```
#####
#
#####

Listen 443

AddType application/x-x509-ca-cert .crt .cer

SSLSessionCache      "shmcb:/private/var/run/ssl_scache(512000)"
SSLSessionCacheTimeout 300

<VirtualHost _default_:443>

    SSLEngine On

    <Location "/si/cc">

        SSLCertificateFile      "/etc/apache2/certs/server.crt"      # Certificado do Servidor
        SSLCertificateKeyFile    "/etc/apache2/certs/server.key"      # Certificado da Chave Privada do Servidor
        SSLCertificateChainFile  "/etc/apache2/certs/cc/ca/caa.crt"  # Cadeia de Certificados do Servidor
        SSLCACertificateFile    "/etc/apache2/certs/cc/ca/caa.crt"  # Certificado da Autoridade de Certificação

        SSLOptions +StdEnvVars +ExportCertData

        SSLVerifyClient require
        SSLVerifyDepth 3

        SSLRequire ( %{SSL_CLIENT_I_DN_CN} in {
            "EC de Autenticação do Cartão de Cidadão 0001",
            "EC de Autenticação do Cartão de Cidadão 0002",
            "EC de Autenticação do Cartão de Cidadão 0003" } )

    </Location>

    AddDefaultCharset UTF-8

</VirtualHost>

#####
```

Figura 5.1: Configurações do Apache para a Autenticação com o Cartão de Cidadão

Desde incompatibilidade da versão dos certificados disponibilizados pela AMA com os servidores Apache e a sua extensão para o OpenSSL, sendo que este último necessita para ser considerado válido que os certificados associados estejam no formato PEM (formato de texto) ao invés do que é disponibilizado em CER (formato binário), até problemas de codificação dos caracteres associados ao certificado, muita coisa aconteceu durante a integração dos métodos disponibilizados pelo CC.

5.5.2 Demonstração

Para efeitos de teste da autenticação com o Cartão de Cidadão no SIGARRA foi criada uma página no ambiente da FEUP, como mostra a figura 5.2. Esta página, apesar de apenas uma versão de teste da funcionalidade, tenta seguir com as normas da AMA sobre a identificação clara de que a autenticação numa página vai ser feita com o uso do CC.

Implementação

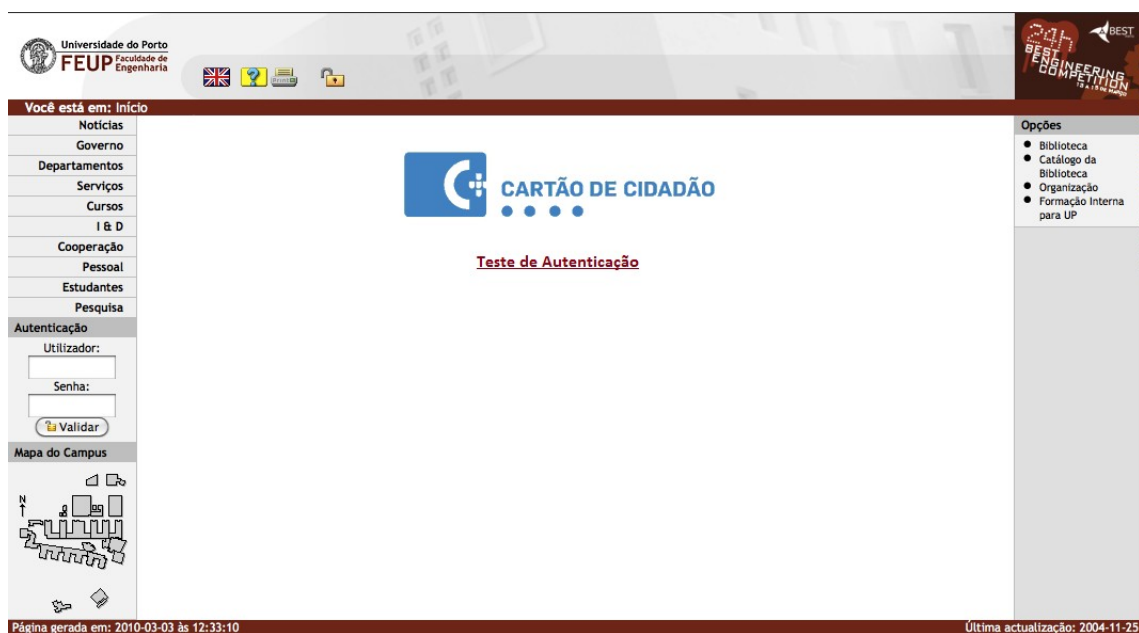


Figura 5.2: Demonstração da Autenticação com o Cartão de Cidadão

Após o utilizador submeter o seu pedido de autenticação ao Apache, este envia um pedido em resposta de volta para o navegador pelos certificados que está à espera de receber do utilizador. Este pedido pode ser visualizado na figura 5.3, onde é mostrada o exemplo da caixa de selecção de certificados do Firefox, onde o utilizador deve identificar o certificado a usar.

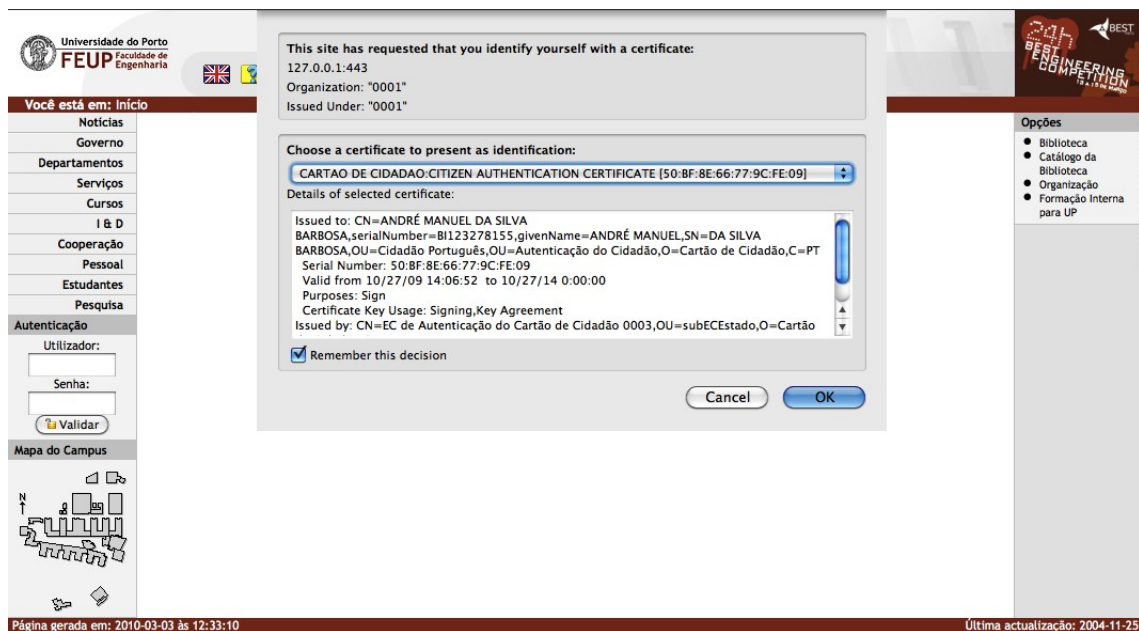


Figura 5.3: Demonstração do pedido do Certificado de Autenticação do Cartão de Cidadão

Implementação

Quando o navegador tentar aceder ao certificado de autenticação do CC, através da camada de interação entre o sistema operativo respectivo e o leitor do cartão, o Middleware do CC, é lhe pedido o respectivo PIN, tal como é ilustrado na figura 5.4. Após a introdução do PIN com sucesso, o navegador recebe o certificado do cartão e envia-o de volta para o servidor.

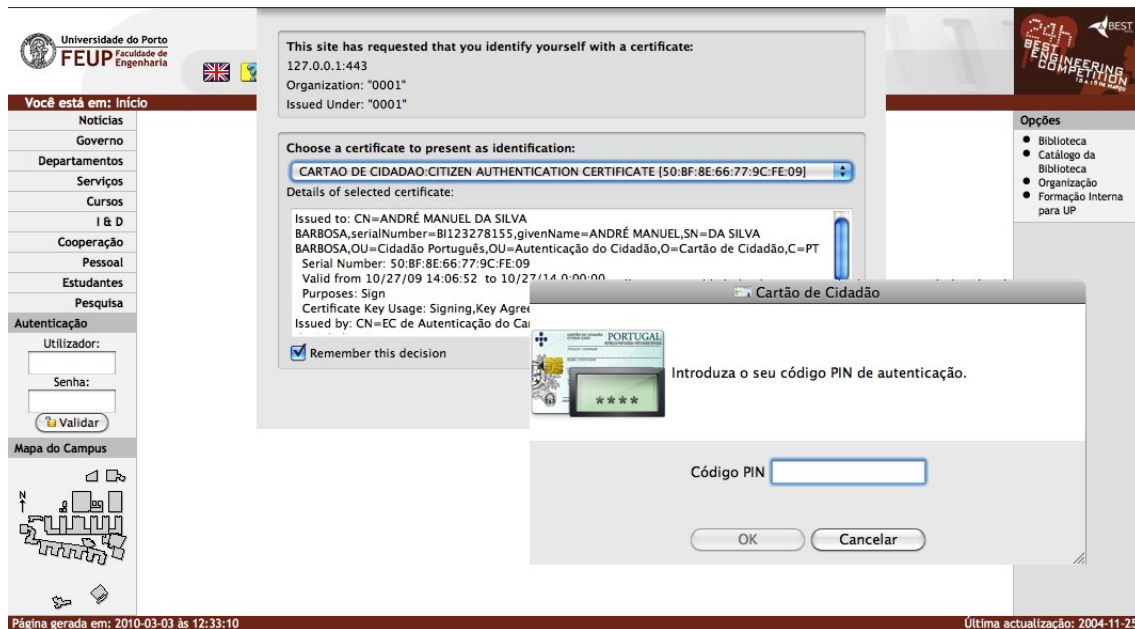


Figura 5.4: Demonstração do pedido de PIN de Autenticação do Cartão de Cidadão

Depois da aceitação do PIN, o sistema acede ao certificado digital de autenticação, e envia os parâmetros SSL associados ao estabelecimento da ligação para o servidor, de acordo com o que é ilustrado na tabela 5.2. Nesta lista de parâmetros podemos então obter todos os dados contidos no certificado de autenticação do meu Cartão de Cidadão e alguns dados da validação ou não do certificado pelo servidor, a começar com `SSL_CLIENT_VERIFY = SUCESS`. Os restantes mostram dados como os meus nomes, número de identificação civil, algoritmos de encriptação das chaves, entidade de certificação e respectivo período de validade do certificado.

Implementação

<i>Parâmetro</i>	<i>Conteúdo</i>
SSL_CLIENT_VERIFY	SUCCESS
SSL_CLIENT_M_VERSION	3
SSL_CLIENT_M_SERIAL	50BF8E66779CFE09
SSL_CLIENT_V_START	Oct 27 14:06:52 2009 GMT
SSL_CLIENT_V_END	Oct 27 00:00:00 2014 GMT
SSL_CLIENT_V_REMAIN	1699
SSL_CLIENT_S_DN	/C=PT/O=Cartão de Cidadão Cidade do Cidadão/OU=Autenticação do Cidadão Cidade do Cidadão/OU=Cidade do Cidadão Portugal/SN=DA SILVA BARBOSA/GN=ANDRÉ MANUEL/serialNumber=BI123278155/CN=ANDRÉ MANUEL DA SILVA BARBOSA
SSL_CLIENT_S_DN_C	PT
SSL_CLIENT_S_DN_O	Cartão de Cidadão
SSL_CLIENT_S_DN_OU	Autenticação do Cidadão
SSL_CLIENT_S_DN_CN	ANDRÉ MANUEL DA SILVA BARBOSA
SSL_CLIENT_S_DN_G	ANDRÉ MANUEL
SSL_CLIENT_S_DN_S	DA SILVA BARBOSA
SSL_CLIENT_I_DN	/C=PT/O=Cartão de Cidadão Cidade do Cidadão/OU=subECEstado/CN=EC Autenticação do Cidadão Cidade do Cidadão 0003
SSL_CLIENT_I_DN_C	PT
SSL_CLIENT_I_DN_O	Cartão de Cidadão
SSL_CLIENT_I_DN_OU	subECEstado
SSL_CLIENT_I_DN_CN	EC de Autenticação do Cartão de Cidadão 0003
SSL_CLIENT_A_KEY	rsaEncryption
SSL_CLIENT_A_SIG	sha1WithRSAEncryption

Tabela 5.2: Parâmetros SSL enviados do Cliente para o Servidor

5.6 Resumo

Infelizmente, a implementação das soluções não cobriu uma grande parte funcional do módulo. Ao invés, foram elaborados testes que comprovam conceitos e abordagens diferentes às funcionalidades em concreto. Muitos são os casos em que uma arquitectura e uma especificação de requisitos bem feitas são sinónimos de sucesso a médio prazo, mais que um vasto número de linhas de código que, mais tarde ou mais cedo, vão sofrer alterações estruturais graves. Era isto

Implementação

que tínhamos em mente, quando decidimos atribuir mais peso no tempo de análise e definição das soluções para os muitos problemas em concreto.

6 Conclusões e Trabalho Futuro

Neste capítulo são feitas as apreciações ao trabalho realizado e as possibilidades em aberto para o futuro.

6.1 Satisfação dos Objectivos

Apesar de não terem sido implementadas todas as funcionalidades analisadas na decorrer do projecto, também é verdade que esse não era especificamente o objectivo. O alvo principal desta dissertação era o estudo dos cenários de utilização do Cartão de Cidadão em sistemas de informação académicos, e esses objectivos sim, foram cumpridos. Mas também não se pode dizer que foram só analisadas soluções, tendo em conta que por exemplo a autenticação foi implementada em conjunto com o SI existente.

Além disso, os modelos de dados definidos transmitem bastante flexibilidade ao cenário de extensões e desenvolvimentos futuros. Foi bastante motivador a percepção de ter contribuído para a melhoria das relações entre o cidadão e as empresas públicas e privadas. Também foi extremamente aliciante a possibilidade de trabalhar com um leque de tecnologias tão vasto na área de segurança e de poder implementar funcionalidades nesse campo.

6.2 Trabalho Futuro

Como ficou bem patente no capítulo de Implementação, ainda há muito trabalho pela frente no sentido de ter um módulo de segurança com todas as funcionalidades desejadas, completamente integradas com o Cartão de Cidadão. Mais ainda, se tivermos em consideração que o projecto do CC não está completo e está em estudo o lançamento para breve de novas potencialidades, nomeadamente na área da biometria e da encriptação. Qualquer que seja o caminho a tomar nesta área é importante nunca esquecer que os dados dos cidadãos devem ser sempre protegidos e nunca publicados sem o consentimento do mesmo. Este é um direito de Cidadão e nunca pode existir um motivo tecnológico que o sobreponha.

Referências

- [CICA01] Faculdade de Engenharia da Universidade do Porto. Centro de Informática Prof. Correia Araújo, de . http://www.fe.up.pt/si/unidades_geral.visualizar?p_unidade=11&P_amo_id=89.
- [CICA02] Faculdade de Engenharia da Universidade do Porto. Visita ao CICA, Março de 2009. http://www.fe.up.pt/si/web_base.gera_pagina?P_pagina=21117.
- [SYNV01] Sysnovare. Empresa, de 2009. http://www.sysnovare.pt/sysnovare/web_base.gera_pagina?p_pagina=126534.
- [CCOB01] Agência para a Modernização Administrativa. Objectivos do Cartão de Cidadão, de 2008. http://www.cartaodecidadao.pt/index.php?option=com_content&task=view&id=18&Itemid=26&lang=pt.
- [CCMN01] Agência para a Modernização Administrativa. Manuais do Cartão de Cidadão, de 2008. http://www.cartaodecidadao.pt/index.php?option=com_content&task=section&id=14&Itemid=100&lang=pt.
- [SPLG01] SAPO. Autenticação no SAPO, de 2009. <https://login.sapo.pt/>.
- [SPSL01] SAPO. Software Livre do SAPO, de 2010. <http://softwarelivre.sapo.pt/>.
- [UPSG01] Universidade do Porto. SIGARRA, Janeiro de 2010. http://sigarra.up.pt/up/web_base.gera_pagina?p_pagina=2418.
- [UPSG02] Faculdade de Engenharia da Universidade do Porto. SIGARRA da FEUP, Abril de 2009. http://www.fe.up.pt/si/web_base.gera_pagina?p_pagina=21181.
- [INCRYP] Network Associates, Inc.. Introduction to Cryptography. , , 2000.
- [HSTCRYPT] Fred Cohen. A Short History of Cryptography . , , 1995.
- [MS246071] Microsoft. Description of Symmetric and Asymmetric Encryption. Outubro de 2007. <http://support.microsoft.com/kb/246071>.
- [FCCN9929] Artur Romão e Miguel Mira da Silva. Um Protocolo para Troca de Mensagens com Garantias Fortes de Não-repúdio. de 1999. <http://www.fccn.pt/crc1999/FINAIS/artigo29/ARTIGO29.HTM>.

Referências

- [WIKIDSIG] Wikipedia. Digital Signature, Março de 2010.
http://en.wikipedia.org/wiki/Digital_signature.
- [WIKITSTP] Wikipedia. Trusted Timestamping, Fevereiro de 2010.
http://en.wikipedia.org/wiki/Trusted_timestamping.
- [MS195724] Microsoft. Description of Digital Certificates. Janeiro de 2007.
<http://support.microsoft.com/kb/195724>.
- [CISSP08] James Michael Stewart, Ed Tittel, Mike Chapple. *CISSP: Certified Information Systems Security Professional Study Guide*. John Wiley and Sons, 2008.
- [CCSTS10] Agência para a Modernização Administrativa. Estatísticas do Cartão de Cidadão, Fevereiro de 2010. http://www.cartaodecidadao.pt/index.php?option=com_content&task=view&id=196&Itemid=103&lang=pt.
- [CCPVC08] Agência para a Modernização Administrativa. Prova de Conteito do Cartão de Cidadão, de 2008. http://www.cartaodecidadao.pt/index.php?option=com_content&task=view&id=20&Itemid=26&lang=pt.
- [CCOBV08] Agência para a Modernização Administrativa. Objectivos do Cartão de Cidadão, de 2008. http://www.cartaodecidadao.pt/index.php?option=com_content&task=view&id=18&Itemid=26&lang=pt.
- [CCCRCT] Agência para a Modernização Administrativa. Características do Cartão de Cidadão, de 2008. http://www.cartaodecidadao.pt/index.php?option=com_content&task=view&id=19&Itemid=29&lang=pt.
- [UPAP09] Universidde do Porto. Breve Apresentação da Universidade do Porto, Abril de 2009. http://sigarra.up.pt/up/web_base.gera_pagina?P_pagina=122225.

Anexo A: Especificações Técnicas do Cartão de Cidadão

Neste anexo são apresentadas as especificações técnicas do Cartão de Cidadão, tanto a nível físico como técnico. Os dados listados aqui foram na sua maioria retirados do manual de requisitos do Cartão de Cidadão elaborado pela Comissão Nacional de Protecção de Dados (CNPd) para consumo interno. Pretende-se que as informações aqui apresentadas sirvam de base para decisões a tomar na implementação de funções de acesso ao cartão.

A.1 Dados do Cartão de Cidadão (frente)

<i>Informação</i>	<i>Dimensão e Tipo de Dados</i>	<i>Motivo de Inclusão</i>
Estado ou Entidade emissora	Texto (máx. 20 caracteres)	Documento de Viagem (ICAO) Identificação Civil
Tipo de Documento ("Cartão de Cidadão")	Texto (máx. 17 caracteres)	Documento de Viagem (ICAO) Identificação Civil Identificação perante os Organismos
Nº de Identificação Civil e Nº do documento (<i>card number</i>)	Dígitos e caracteres (máx. 14 caracteres) Nº Id. Civil: 8 dígitos Nº documento: nº id. Civil + 2 caracteres + <i>check digit</i> documento Formato de impressão:	Identificação Civil Documento de Viagem (ICAO) Ciclo de vida do cartão CWA 15264-1

Referências

	DDDDDDDDb-bAAC Onde: <i>b</i> - espaço em branco A – [Z.. A, 9.. 0] C – <i>Check Digit</i> [0.. 9] Nota: Não obstante pretender-se que estes números sejam representados em conjunto, a representação visual deverá ser tal que o cidadão comum distinga facilmente o nº de identificação civil e entenda que os restantes caracteres não fazem parte deste.	
Data de validade do cartão	Dígitos e caracteres (máx. 15 caracteres) Formato definido pela ICAO: DDbMMbAAAA <i>b</i> - espaço em branco	Documento de Viagem (ICAO) Identificação Civil
Apelidos do cidadão	Texto (máx. 110 caracteres, podendo ocupar até três linhas)	Documento de Viagem (ICAO) Identificação perante todos os Organismos
Nomes próprios do cidadão	Texto (máx. 50 caracteres, podendo ocupar até três linhas)	Documento de Viagem (ICAO) Identificação perante todos os Organismos
Sexo	Texto (máx. 3 caracteres) Formato: ‘F’ (feminino), ‘M’ (masculino), ‘X’ (informação não especificada)	Documento de Viagem (ICAO)
Nacionalidade	Texto (máx. 3 caracteres) Valores definidos pela ICAO: “PRT” para cidadãos de nacionalidade portuguesa;	Documento de Viagem (ICAO)

Referências

	“BRZ”, para cidadãos de nacionalidade brasileira ao abrigo do Tratado de Porto Seguro.	
Data de Nascimento	Dígitos e caracteres (máx. 15 caracteres) Formato definido pela ICAO: DDbMMbAAAA Onde: b - espaço em branco	Documento de Viagem (ICAO) Identificação Civil Identificação STAPE Identificação Saúde Identificação Segurança Social
Altura	Texto (4 alfanuméricos) Formato para altura em metros: D,DD onde D - dígito	Identificação Civil
Fotografia Digitalizada	Imagem a preto e branco, segundo normas ICAO (Doc 9303, Parte 3, Secção 3)	Documento de Viagem(ICAO) Identificação Civil
Assinatura Digitalizada	Imagem a preto e branco, segundo normas ICAO	Documento de Viagem (ICAO) Identificação Civil Identificação STAPE

A.2 Dados do Cartão de Cidadão (verso)

<i>Informação</i>	<i>Dimensão e Tipo de Dados</i>	<i>Motivo de Inclusão</i>
Informação da nacionalidade	Texto (máx. 160 caracteres) Cidadão Português/ Portuguese Citizen Para cidadãos de nacionalidade brasileira ao abrigo do Tratado de Porto Seguro colocar: “Cidadão Brasileiro ao abrigo do Tratado Porto Seguro/ [DESCRITIVO EM INGLÊS]”.	

Referências

	Nota: Este descritivo será oportunamente definido em sede de projecto.	
Filiação – mãe	Texto (máx. 160 caracteres)	Identificação Justiça
Filiação – pai	Texto (máx. 160 caracteres)	Identificação Justiça
Número de Identificação Fiscal (NIF)	Dígitos (9 dígitos)	Identificação Finanças
Número de Identificação da Segurança Social (NISS)	Dígitos (11 dígitos)	Identificação Segurança Social
Número de Utente da Saúde	Dígitos (9 dígitos)	Identificação Saúde
Informação para leitura óptica (MRZ – <i>machine readable zone</i>)	Regras definidas pela ICAO (3 linhas de 30 caracteres OCR-B) Para cidadãos de nacionalidade brasileira ao abrigo do Tratado de Port Seguro, o Cartão de Cidadão não serve como documento de viagem. Assim, e em detrimento da MRZ, a zona de leitura óptica deverá conter apenas a seguinte indicação: “Não serve de documento de viagem/Not a Travel Document ”	Documento de Viagem (ICAO)
Nº de versão do cartão	O nº de versão do Cartão deverá ser visível para o Cidadão, agrupando num único campo dígitos e caracteres (15) Formato: AA.AAAA.AA.AA.A Onde: - Primeiro conjunto (2 elementos) corresponde às versões gráfica e de segurança; - Segundo conjunto (4 elementos) corresponde à versão de S.O. do <i>chip</i>; - Terceiro conjunto (2 elementos) corresponde às aplicações	Ciclo de Vida do Cartão

Referências

	existentes no <i>chip</i>; - Quarto conjunto (2 elementos) corresponde a características do <i>chip</i>; - Quinto conjunto (1 elemento) corresponde à geração do formato do número de versão.	
--	--	--

A.3 Modelo de Dados a incluir no chip do Cartão de Cidadão

<i>ID</i>	<i>Informação</i>	<i>Dimensão e Tipo de Dados</i>	<i>Motivo de Inclusão</i>	<i>Visível</i>	<i>Chip</i>
Dados Específicos do Cartão					
1	Entidade emissora do cartão	Texto	• Documento de Viagem (ICAO) • CWA 15264-1 • Identificação Civil	S	S
2	Estado (nome do país)	Texto	• Documento de Viagem (ICAO) • CWA 15264-1 • Identificação Civil	S	S
3	Tipo de Documento	Texto	• Documento de Viagem (ICAO) • Identificação Civil • Identificação perante os outros Organismos	S	S
4	Nº do documento (<i>card number</i>)	Texto	• Documento de Viagem (ICAO) • Ciclo de vida do cartão • CWA 15264-1	S	S
5	Nº de série do cartão (PAN - <i>primary account number</i>)	Dígitos	• Ciclo de vida do cartão • PAN segundo CEN/TS 15480 (<i>draft</i>)	N	S
6	Nº de versão do cartão e <i>chip</i>	Texto	• Ciclo de vida do cartão	S	S

Referências

7	Data de emissão do cartão	Dígitos	• Identificação Civil • CWA 15264-1	N	S
8	Local de pedido do cartão	Texto	• Identificação Civil	N	S
9	Data de Validade do Cartão	Dígitos	• Documento de Viagem (ICAO) • CWA 15264-1 • Identificação Civil	S	S
10	Chave privada do cartão	Binário CVC	• Autenticação mútua e comunicação segura entre o cartão e aplicações externas (Sistema de Ciclo de Vida).	N	S
11	Chave pública do cartão	Binário CVC	• Autenticação mútua e comunicação segura entre o cartão e aplicações externas (Sistema de Ciclo de Vida).	N	S
Dados comuns do Cidadão (dados de identificação)					
12	Apelidos do cidadão	Texto	• Autenticação mútua e comunicação segura entre o cartão e aplicações externas (Sistema de Ciclo de Vida).	S	S
13	Nome próprio do cidadão	Texto	• Documento de Viagem (ICAO) • CWA 15264-1 • Identificação perante todos os Organismos	S	S
14	Sexo	Texto	• Documento de Viagem (ICAO) • CWA 15264-1	S	S
15	Nacionalidade	3 caracteres (código ICAO)	• Documento de Viagem (ICAO) • CWA 15264-1	S	S
16	Data de Nascimento	Data	• Documento de Viagem (ICAO) • CWA 15264-1 • Identificação perante os vários Organismos	S	S

Referências

17	Altura	Número, 3 dígitos	• Identificação Civil	S	S
Dados biométricos do Cidadão – fotografia / impressões digitais					
18	Fotografia Digitalizada	n.a.	• Documento de Viagem (ICAO) • Identificação Civil	S	N
19	Fotografia Digitalizada	Binário (CBEFF e imagem <i>token frontal</i> ou <i>full frontal</i> em cores, segundo normas ISO)	• Documento de Viagem (ICAO)	N	S
20	Template de impressão digital indicador esquerdo (ou dedo alternativo)	Binário (CBEFF e <i>template</i> segundo normas ISO)	• Autoridades policiais	N	S
21	Template de impressão digital indicador direito (ou dedo alternativo)	Binário (CBEFF e <i>template</i> segundo normas ISO)	• Autoridades policiais	N	S
Morada de residência					
22	Morada de residência	Estrutura (definida mais adiante)	• Identificação Civil	N	S
22-a	Nº de geração da morada	6 dígitos (ano e 2 dígitos sequenciais)	• Processo de actualização de morada no <i>chip</i> (em múltiplos Organismos)	N	S
Dados sectoriais da Justiça					
23	Nº de identificação civil + <i>check Digit de BI</i>	9 dígitos	• Documento de Viagem (ICAO) • Identificação Civil	S	S
24	Assinatura Digitalizada	Binário (imagem em tons cinzento)	• Documento de Viagem (ICAO) • Identificação Civil • Identificação STAPE	S	N
25	Filiação - apelidos da mãe	Texto	• Identificação Justiça	S	S

Referências

26	Filiação – nomes próprios da mãe	Texto	• Identificação Justiça	S	S
27	Filiação - apelidos do pai	Texto	• Identificação Justiça	S	S
28	Filiação – nomes próprios do pai	Texto	• Identificação Justiça	S	S
29	Indicações Eventuais	Texto	• Identificação Justiça	N	S
Dados sectoriais das Finanças					
30	Nº de Identificação Fiscal (NIF)	9 dígitos	• Identificação Finanças	S	S
Dados sectoriais das Segurança Social					
31	Nº de Identificação da Segurança Social (NISS)	11 dígitos	• Identificação Segurança Social	S	S
<i>Dados sectoriais da Saúde</i>					
32	Nº de Utente da Saúde	9 dígitos	• Identificação Saúde	S	S
Certificados digitais do cidadão					
33	Certificado digital para autenticação segura	Binário X.509v3	• CEN Workshop Agreement 15264-1 (documento de referência para uma arquitectura de um sistema europeu de eId interoperável)	N	S
34	Certificado digital para assinatura electrónica qualificada	Binário X.509v3	• Decreto-lei 62/2003 de 3 de Abril de 2003, Decreto-lei 290-D/99 de 2 de Agosto de 1999 • CEN Workshop Agreement 15264-1 (documento de referência para uma arquitectura de um sistema europeu de eId interoperável)	N	S
Certificados digitais e chaves criptográficas de entidades					
35	Certificado digital com chave pública da Entidade de Certificação de Documentos do Cartão de Cidadão (<i>document signer</i>)	Binário X.509v3	• Modelo de PKI Nacional, em estudo pela Entidade de Certificação Electrónica do Estado • Recomendações para uma PKI nacional, Fevereiro 2005, Estrutura Nacional de	N	S

Referências

			Segurança da Informação		
36	Certificado digital com chave pública da Entidade de Certificação <i>Root</i> do Cartão de Cidadão (CA <i>root</i>)	Binário X.509v3	• Modelo de PKI Nacional, em estudo pela Entidade de Certificação Electrónica do Estado • Recomendações para uma PKI nacional, Fevereiro 2005, Estrutura Nacional de Segurança da Informação	N	S
43	Certificado ou certificados com chave(s) pública(s) de sub- CA(s) de controlo de acessos ao <i>chip</i>	Binário CVC	• Autenticação de Sistemas de Informação de Organismos perante o Cartão	N	S
Dados personalizáveis					
42	Pasta pública do cidadão	Texto (comprimento máximo a definir em função do espaço disponível no <i>chip</i>)	• Flexibilização do uso pelo cidadão – permitir colocação dos dados que o cidadão desejar	N	S

Índice Remissivo

A

ACD, 46, 49, 61
ADQ, 53, 54, 61
AJAX, 48
AMA, 3, xv, 17, 35, 36, 45, 46, 51
Apache, 5, 44, 45, 60
API, i, iii, xv, 23, 43, 48, 54, 59, 61, 62, 66
applet, 23, 44, 48, 51, 60
Applet, 23
autoridade de certificação, 13, 45
Autoridade de Certificação, 14-16

C

CER, 45
chave privada, 10, 11, 13, 15, 51, 55-57
chave pública, 10-12, 14-16, 55, 56
CICA, 2, 7, xv, 31
CNPd, xv, 34, 50, 77
criptografia, 5, 8-11, 43
Criptografia, 8
CRL, xv, 17
CSS, 7, xv
CVC, 20

D

DAS, 11
DES, 10, xv
DOCX, 51

E

EAS, 10
EC, xv, 20, 45
Eclipse, 8

eid, 60

eID, xv, 23, 60

EIE, 56, 57, 59, 61

criptação assimétrica, 10, 11

Encriptação Assimétrica, 10

criptação simétrica, 9

Encriptação Simétrica, 9

F

FEUP, 1-3, 6, vii, xv, 24, 27, 29, 31, 33, 41, 45

G

GESSI, 5, 7, xv, 45, 60-62

Google Code, 8, 60

GP, 7, xv

H

hash, 11-13

Hash, xvi

HTTP, 5, xv

I

ICP, xv, 16

iText, 23, 51

J

Java, 6, 8, 22, 23, 44, 48, 49, 60, 62, 66

JavaScript, xv

M

MD5, 13

MIEIC, 1, xvi

MSA, xvi, 43, 46, 49, 53, 54, 56, 57, 59-62, 66, 67

O

OAS, xv, 16, 23, 24

Índice Remissivo

OCSF, xvi, 17, 20

ODT, 51

OpenID, 21

OpenSSL, 45

Oracle, 5, 7, xv, 16, 22-25, 36, 40, 52, 58

P

PDF, xvi, 23, 50, 51

PEM, xvi, 45

PKCS#11, 60

PKI, xv-17, 20

PL/SQL, 5-7, 22, 60, 62, 66

PTEID4J, 60-62, 67

PTEIDLIB, 60, 62

R

RSA, 11, xvi

S

SAPO, 3, 21, 22

SCEE, xvi, 20

SHA-1, 13

SHA-2, 13

SIGARRA, 1, 2, 5-viii, xvi, 45, 60

SQL, 5-vii, xvi, 22, 60, 62, 66

T

TDE, 24, 25

timestamp, 20

Timestamp, 13

TSA, 13, xvi

U

UML, xvi

UP, 1, 2, 6, vii, xvi, 27, 28, 31, 39, 41, 44, 45

X

X.509, 17

XML, xvi, 52

XMLDsig, 52