UNIVERSIDADE DA BEIRA INTERIOR
Covilhã | Portugal

Ticket-ID

Arquitectura Móvel para a Integração de Serviços de Comércio Electrónico, Comunicação NFC e a Segurança do Cartão de Cidadão.

Vasco André Gonçalves Nicolau

Submetida à Universidade da Beira Interior para
obtenção do grau de Mestre em Engenharia Informática

Orientado pelo Professor Doutor Paul Andrew Crocker
Co-Orientado pelo Mestre José Eduardo Pina Miranda - (Multicert)

Departamento de Informática
Universidade da Beira Interior
Covilhã, Portugal
http://www.di.ubi.pt

Agradecimentos

A realização desta dissertação só foi possível graças à colaboração de várias pessoas. Quero manifestar o meu agradecimento e dedicação a todas elas.

Em primeiro lugar queria agradecer à minha querida namorada, Vanessa Cruz, por todo o apoio, força, motivação, paciência e dedicação incansável comigo ao longo de todo o percurso universitário.

Quero também agradecer à minha família por todo o apoio e esforço que fizeram para que eu tirasse um curso superior e, pelo orgulho que sentem por mim.

A todos os meus amigos por toda a cooperação dada ao longo do curso.

Ao Professor Paul Crocker por toda a paciência, disponibilidade de tempo e acima de tudo pelos seus ensinamentos e conselhos, que foram cruciais ao longo do percurso académico.

Ao Professor Simão Melo de Sousa pela confiança depositada em mim e por todos os momentos de apoio e incentivo ao longo do curso.

Agradecer ainda ao ***Instituto de Telecomunicações***(IT) e ao ***RELiablE And SEcure Computation Group***(Release) pelo apoio imprescindível que me foi dado.

Por último, à empresa ***Multicert*** em especial ao Mestre José Pina Miranda por todo o apoio incondicional dado ao longo do desenvolvimento de toda a dissertação.

A todos vocês bem-haja!

Resumo

A presente dissertação resulta da investigação de diversas tecnologias, tendo como objectivo a criação dum projecto inovador tanto na vertente tecnológica como comercial que incentivasse o uso principalmente do Cartão de Cidadão e a tecnologia *Near Field Comunication* no contexto das comunicações moveis, a este projecto inovador deu-se o nome de ***Ticket-ID***. O sistema resultante foi idealizado de modo a usufruir das melhores características de cada tecnologia de forma a ser possível englobar as mesmas num todo de forma segura, simples e inovadora.

Assim, o projecto ***Ticket-ID***, consiste numa plataforma informática inovadora que se integra no campo da bilhética, tendo em conta todas as fases do processo de reserva, aquisição e validação de bilhetes. Esta engloba diversas tecnologias, como o *NFC*, *GSM*, *QR-Code*, Biometria e a Computação Móvel com o objectivo de proporcionar um sistema comprovadamente seguro, flexível, inovador, simples e viável comercialmente.

O principal objectivo da utilização do Cartão de Cidadão consiste em fortalecer o sistema de bilhética do ponto de vista da identificação e autenticação pessoal. Desta forma é possível elaborar um sistema resiliente, associado à identidade digital do cidadão ao longo do ciclo de vida dos bilhetes. Para atingir este objectivo foi necessário desenvolver um novo *middleware* para o cartão de cidadão.

A solução proposta perspectiva-se que desperte o interesse e a interactividade dos cidadãos devido à originalidade proporcionada. Almeja-se que contribua significativamente para o aumentando da fiabilidade de soluções de bilhética móveis, graças à utilização inovadora da identidade digital proporcionada pelo Cartão de Cidadão.

Abstract

This dissertation is the result of investigation in various technologies whose objective principal is the creation of a technologically and commercially innovative project that encourages the use of the electronic identification card, *Citizens Card*, and *Near Field Communication* in the context of mobile communications and payments. This innovative project was given the name *Ticket-ID*. The resulting project was designed to use the best characteristics of each technology encompassing them all in a system that would be secure and at the same innovative.

Ticket-ID is therefore a new computing system for electronic ticketing which covers the entire tickets lifecycle, all the stages of the booking, purchasing and validation of the tickets. The technologies used include NFC and *GSM communications*, the *QR-Code format*, *Biometrics* and *Mobile Computing* with the overall aim of designing and prototyping a safe, *secure*, *flexible*, innovative and commercially viable project.

One of the principal contributions of this thesis is the way that the *Citizens Card* is integrated into the security layer of the proposed architecture. The main use of the *Citizens Card* is to strengthen the ticketing system from the viewpoint of personal identification and authentication. Thus it is possible to develop a resilient system, associated with the digital identity of citizens throughout the life cycle of tickets. In order to achieve this a new *Middleware* for the *Citizens Card* was also developed.

The proposed system, *Ticket-ID*, aims to arouse the interest and interactivity of citizens and companies due to its originality and novelty. One hopes that this thesis contributes significantly to increasing the reliability of mobile ticketing solutions due to the innovative use of a digital identity provided by the *Citizen Card*.

Palavras-Chaves

Cartão de Cidadão, Segurança, Autenticação, Validação, Assinatura, Pagamentos, Qr-Code, NFC, Identidade electrónica, e-Ticket, Middleware.

Keywords

Citizen Card, Security, Mobile, Authentication, Validation, Signature, Payments, Qr-Code, Near Field Comunication, Electronic Identity, e-Tickets, Middleware.

Acrónimos

AMA Agência para a Modernização Administrativa

APDU Application Protocol Data Unit

API Application Programming Interface

ATR Answer to Reset

BD Base de Dados

e-ID Electronic Identity

GSM Global System for Mobile Communications

IAS Identification, Autentication and digital Signature

ISO International Organization for Standardization

MNO Mobile Network Operator

MMS Multimedia Messaging Service

MoC Match On Card

MS Microsoft

NFC Near Field Communcation

Otp One time password

PC/SC Personal Computer/Smart Card

PIN Personal identification number

PKCS Public-key Cryptography Standards

Pki Public-key infrastructure

QR-Code Quick Response - Code

RFID Radio-Frequency IDentification

SDK Software Development Kit

SIBS Sociedade Interbancária de Serviços

Stork Secure idenTity acrOss boRders linKed

SMS Short Message Service

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Com o surgimento das novas tecnologias de informação e comunicação (TIC), o comércio electrónico tem crescido imenso sendo este impulsionado pela Internet, contudo estão-lhe associados diversos perigos para a sociedade, como o cibercrime, a ciberguerra e a criminalidade em geral. Portanto é cada vez mais importante garantir a nossa segurança e a nossa privacidade na sociedade de informação, principalmente no contexto das vendas e transacções electrónicas na compra de produtos ou serviços, uma vez que se assiste a uma constante desmaterialização de documentos físicos por documentos electrónicos.

Por outro lado, as novas TIC permitem a facilidade, rapidez e automação de operações que a sociedade impõe. Como consequência, esta mudança para o mundo digital pode gerar a sensação de insegurança ou a facilidade de usurpação e transmissão dos dados.

Tendo em conta que a segurança é tida como um elemento essencial de qualquer sistema, a prova de conceito deste projecto assenta sobre os princípios de segurança que um sistema de bilhética, mais precisamente a venda de bilhetes *Online* e a posterior validação dos mesmos, deve contemplar.

Surge assim, o projecto *Ticket-ID*, que consiste numa plataforma que engloba diversas tecnologias, como o *smart card*, *NFC*, *GSM*, Código de Barras, Biometria e a Computação Móvel, que visam sobretudo proporcionar um sistema de bilhética com características inovadoras de simples compressão e de rápida utilização.

Importa ainda referir que um ponto fundamental do projecto consiste na camada de segurança. Esta será capaz de associar a segurança da identidade digital, proporcionada pelo cartão de cidadão, ao ciclo de vida dos bilhetes.

A introdução do cartão de cidadão e a originalidade da sua utilização vem assim potenciar um novo sistema, inovador, fortemente seguro e de simples utilização. Tendo em consideração a insegurança sentida pela sociedade em alguns sistemas de segurança oferecidos por terceiros, surge assim o cartão de cidadão como um elemento de confiança para a sociedade, o que por si só fará com que as pessoas confiem e tenham interesse em utilizar o mesmo em sistema onde a segurança é vista como um bem essencial.
Assim, a sua contribuição é fulcral no projecto, uma vez que um dos objectivos passa por permitir que a identidade pessoal seja associada à compra de um produto, assinalando com a identidade pessoal um produto intangível.

1.1 Motivação

A sociedade actual é bastante receptiva às novas tecnologias. O facto da tecnologia estar em constante evolução faz com que exista uma competitividade diária na procura e desenvolvimento de novos serviços.

Desde o surgimento do telemóvel, o quotidiano de qualquer cidadão tem vindo a conhecer inúmeras alterações nos seus hábitos diários. Os telemóveis contemplam cada vez mais a tecnologia actual e consequentemente novos serviços. Actualmente estão a ser desenvolvidas novas tecnologias que permitem que o telemóvel seja utilizado para a compra de bilhetes de espectáculos, pagamentos de serviços em substituição dos cartões bancários e a substituição de cartões de fidelização, entre outros.

A inovação tecnológica é sem dúvida um factor determinante para que os consumidores procurem novos produtos tecnológicos reflectindo-se num crescimento económico a nível mundial.

Após uma análise detalhada do mercado dos telemóveis, detectou-se que num futuro próximo a nova funcionalidade que o telemóvel irá acoplar será o de porta-moedas (carteira electrónica) [79] [23] [25]. Será possível através do telemóvel efectuar pagamentos de produtos, usufruir de transportes públicos, reservar e validar bilhetes de espectáculos, entre muitos outros serviços.

Existem a decorrer alguns projectos-piloto que visam sobretudo testar a viabilidade do telemóvel neste contexto [74] [15] [26] [81] [80].

A tecnologia usada nestes projectos-piloto, *NFC*, ainda não está disponível nos telemóveis comercializados actualmente. Espera-se que em meados de 2011, cerca de 30% do mercado dos telemóveis possuam a tecnologia *NFC*, permitindo as transacções sem-fio (*Contactless*).

Deste modo, após uma análise detalhada dos projectos-piloto e da possível integração dos sistemas de pagamento ou de bilhética conhecidos, surgem inúmeras questões relacionadas com a arquitectura dos sistemas propostos e os défices de segurança associados aos mesmos[57] [19], tais como:

- A necessidade de criar pontos de venda em todas as regiões geográficas onde exista possibilidade de venda pode trazer custos elevados ao prestador do serviço. Ainda assim, caso o número de pontos de venda seja reduzido existe o problema da grande afluência de pessoas, criando filas de espera de grande dimensão.
- Procedimentos capazes de efectuar a recuperação de bilhetes perdidos.
- Na maioria dos casos, não existem meios de protecção para monitorizar a utilização não autorizada do bilhete em caso de extravio, furto ou perda.
- Em outros casos, a utilização de mecanismos de segurança forte que combina o PIN pessoal com One-Time-Password em *tokens-USB*, relevam-se na prática pouco viáveis, pois implica que as pessoas transportem mais um objecto pessoal para além da sua utilização ser mais complexa.
- Passiveis ataques a telemóveis, através de vírus e *trojans* são também aspectos sensíveis a ter em consideração.

Tendo cientes as necessidades do mercado e os défices de segurança dos sistemas actuais identificou-se a oportunidade de desenvolver um sistema inovador baseado

na utilização do telemóvel como portador de bilhetes [31]. O sistema é semelhante aos projectos-piloto desenvolvidos, mas possuirá características inovadoras capazes de responder de forma **segura e eficaz** às reais necessidades e desafios impostos pela sociedade. Importa ainda referir que o sistema deve ser visto como um sistema similar aos existentes no mercado da bilhética. Contudo este não se apresenta como um concorrente às soluções existentes de grandes empresas (Gemalto, Vodafone, G&D, Oberthur, VivoTech, ...). Pretende-se sim, apresentar uma alternativa que se fundamenta na camada de segurança mais completa, simples e segura.

Desta forma, decidiu-se utilizar o cartão de cidadão enquanto documento electrónico capaz de dar as respostas necessárias, integrado-o na camada de segurança do sistema, tal como mostra a figura 1.1.

Como tal, a utilização do cartão de cidadão na camada de segurança do sistema é o elemento mais motivador para o desenvolvimento do sistema devido as potencialidades associadas ao mesmo. A sua componente electrónica (*smart card*), enquanto identidade digital, associa-se na perfeição aos ideais de confiança e segurança que um cidadão almeja num sistema desta dimensão. Como exemplo inspirador e bem sucedido é o caso da Estónia, onde a utilização do cartão de cidadão é aplicada em inúmeros serviços públicos e privados [28].

Figura 1.1: Ilustração do sistema.

1.2 Objectivos

Este sistema foi desenhado com o intuito de atingir os seguintes objectivos que se passam agora a listar:

O principal objectivo do projecto consiste em fazer uso das potencialidades oferecidas pelo cartão de cidadão como *smart card*. Nomeadamente no processamento de operações electrónicas, através da segurança da autenticação forte, da assinatura electrónica [51] [52], e ainda no processo de validação da titularidade do documento apresentado [75], estando estas funcionalidades disponíveis através do *chip* do cartão.

Assim, a utilização do cartão de cidadão é um elemento fundamental para assegurar a camada de segurança do sistema que contempla a validação dos bilhetes de forma simples ou forte, consoante as características do serviço.

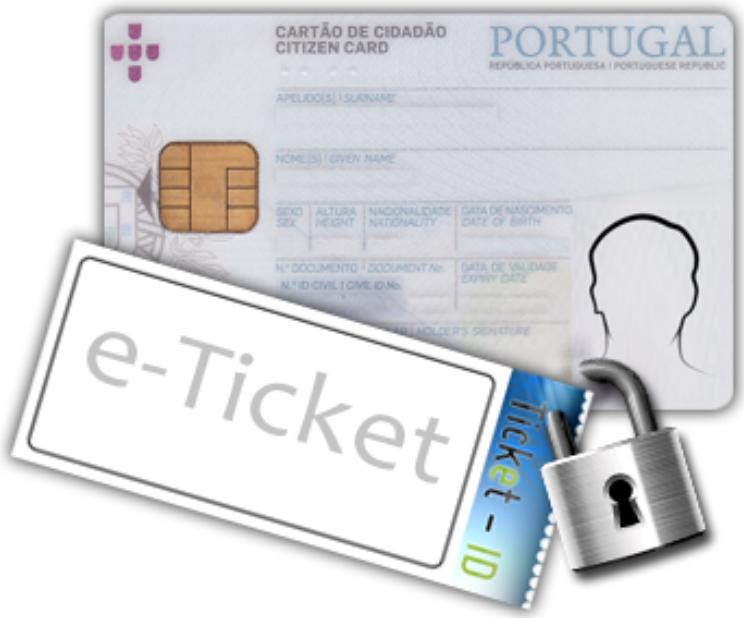

Figura 1.2: Bilhete seguro.

Em segundo lugar, a plataforma deverá que possuir pequenos módulos que representam as entidades que fazem parte do sistema, nomeadamente o agente de venda, o agente de pagamento e o comerciante. Esta repartição em módulos visa sobretudo automatizar ao máximo o fluxo da informação entre todas as entidades, de forma a possibilitar a reserva, aquisição e validação dos serviços de forma rápida, segura eficaz.

Por último, no final espera-se que o produto venha a ser testado e utilizado em ambientes reais, promovendo a competitividade nacional no desenvolvimento de soluções e serviços que utilizem o cartão de forma original. Desta forma é possível enaltecer o valor acrescido em termos de modernização e inovação dos serviços proporcionados pela nova dimensão da identidade nacional. Mais precisamente almeja-se que possa provar o seu valor e consequentemente fazer jus à prova de conceito que se baseia na segurança dada pela identidade digital ao bilhete e mostrar ainda os benefícios do sistema.

1.3 Abordagem

O projecto abordou-se de forma faseada de acordo com a obtenção de informações essenciais ao desenvolvimento do projecto. Inicialmente investigaram-se os produtos similares de aquisição e validação de bilhetes, por forma a serem evidenciadas as potencialidades e os pontos fracos dos mesmos.

Seguidamente, investigaram-se as potencialidades das novas tecnologias usadas em projectos-piloto similares. O objectivo consistiu em determinar se a utilização das tecnologias usadas apresentam uma componente inovadora capaz de ser socioeconomicamente viável na sociedade.

Após, a análise dos produtos similares e das tecnologias a utilizar, elaborou-se uma investigação exaustiva ao cartão de cidadão de forma a perceber as potencialidades deste enquanto elemento fundamental da segurança do sistema.

Esta fase contou com ainda com a preciosa colaboração da *MultiCert*, com o objectivo de ser desenvolvido um produto original e economicamente viável, capaz de responder às necessidades emergentes no mercado.

1.4 Resultados e Divulgação

Desta investigação resultaram novas formas de comunicar com o cartão de cidadão o que permitiu desenvolver uma metodologia capaz de ser utilizada no desenvolvimento de novas funcionalidades.

A presente investigação deu origem à publicação dos artigos, *A Nova Dimensão da Entidade Electrónica em Portugal - I Congresso Nacional de Segurança e Defesa* e *Sniffing with the Portuguese Identify Card for fun and profit - 9th European Conference on Information Warfare and Security*, ambos resultaram no amadurecimento de ideias fundamentais para a elaboração e idealização do sistema desenvolvido.

1.5 Organização do documento

Este documento divide-se em vários capítulos que mostra o processo sequencial da investigação desenvolvida.
Neste primeiro capítulo descreveu-se o projecto, as motivações que levaram ao seu desenvolvimento e os objectivos que se pretendem alcançar no final.
Seguidamente descreve-se o que tratam os próximos capítulos.

Capítulo 2 - Estado da Arte
No próximo capítulo apresenta-se uma descrição sobre as tecnologias utilizadas no projecto e as potencialidades associadas.

Capítulo 3 - Estudo e análise de sistemas relacionados
O terceiro capítulo apresenta o estudo e a análise realizada sobre sistemas relacionados, descrevendo em pormenor o conjunto dos intervenientes na área da bilhética.

Capítulo 4 - *Ticket-ID* projecção e idealização do sistema
O quarto capítulo apresenta a idealização do sistema e os respectivos objectivos a atingir na sua implementação.

Capítulo 5 - Arquitectura do Sistema
O quinto capítulo descreve o sistema de um modo geral, permitindo perceber o real funcionamento do sistema em cada uma das fases.

Capítulo 6 - Engenharia reversa sobre dispositivos criptográficos portáteis
O sexto capítulo descreve a metodologia seguida ao longo do desenvolvido do sistema, com principal incidência no *middleware* desenvolvido para o cartão de cidadão português.

Capítulo 7 - Resultados
No sétimo capítulo apresentam-se os resultados obtidos no sistema *Ticket-ID*, sendo possível observar algumas imagens do sistema em funcionamento e as principais funcionalidades.

Capítulo 8 - Análise do sistema *Ticket-ID*
O oitavo capítulo apresenta uma análise comparativa entre um caso de estudo e o sistema projectado.

Capítulo 9 - Conclusão e trabalho futuro
O último capítulo, consiste em tecer algumas considerações sobre o projecto desenvolvido. Apresentam-se ainda algumas conclusões sobre a camada de segurança baseada no cartão de cidadão. Por fim, descrevem-se as futuras etapas do projecto.

Capítulo 2

Estado da arte

Este capítulo proporciona uma visão geral sobre os actuais sistemas emergentes no campo da bilhética e a segurança associada às novas tecnologias envolvidas nesta área. Seguidamente, efectua-se uma descrição mais especifica sobre as tecnologias, *GSM*, *Código Barras*, *NFC* e *smart cards*, dada a sua importância no sistema projectado.

2.1 Perspectiva geral sobre as novas tecnologias

2.1.1 Novas tecnologias de informação e comunicação

A evolução das Novas Tecnologias de Informação e Comunicação (NTICs) têm aumentado significativamente sobretudo desde a década de 90 a quando da revolução informacional. Estas vieram tornar menos palpável o conteúdo da informação, sendo esta difundida por meio digital/virtual. A forma como foram utilizadas por governos, empresas, indivíduos e sectores sociais possibilitou o surgimento da "sociedade da informação".

Actualmente assiste-se a um aumento significativo da utilização de sistemas computorizados, como o telemóvel, por grande parte da sociedade. O telemóvel é visto pelos cidadãos como um pertence insubstituível e indispensável. Apesar da sua função ser essencialmente para realizar chamadas de voz e enviar mensagens de texto, são constantemente adicionados novos serviços no telemóvel quer pelo fabricante, operador ou terceiros.

Hoje em dia graças aos recursos oferecidos pelos telemóveis, a grande maioria dos utilizadores guarda informações pessoais no mesmo, tais como: as notas e calendários pessoais, fotografias, contactos e até mesmo informação relativa a cartões de crédito e passwords. Dada a importância inquestionável do telemóvel na sociedade, muito provavelmente num futuro próximo, será possível pagar as compras, impostos ao Estado, efectuar a comprar de bilhetes ou até mesmo eleger um presidente ou abrir uma conta num banco. Como consequência desta evolução, os telemóveis serão no futuro vistos como dispositivos portadores da identidade pessoal que se encontra em constante mobilidade, conectividade e actualização informativa.

2.1.2 O telemóvel e a identidade

Tendo em conta estes factos realizou-se uma análise mais cuidada sobre o impacto do telemóvel na sociedade, mas neste caso sem a camuflagem das potencialidades oferecidas pelas novas tecnologias associadas ao mesmo. Exemplo disso é a utilização do telemóvel com acesso, via Internet, às entidades bancárias, permitindo ao utilizador efectuar diversas operações [67] [66].

Neste cenário, em termos de segurança, existe uma difícil tarefa de autenticar os utilizadores remotamente e fornecer um nível adequado de aceitação e de não-repúdio nas transacções. Isto deve-se em grande parte ao facto da esmagadora maioria das soluções actuais serem baseadas em infra-estruturas mantidas pelos operadores de rede móvel ou pelas instituições financeiras [49].

Assim, face ao elo de ligação entre a tecnologia e a identidade, torna-se necessário analisar a segurança e os riscos associados, uma vez que, existe uma percepção diminuta acerca dos riscos a que o utilizador está exposto. A forma mais simples de se constatarem estes riscos, é de forma análoga aos ataques direccionados aos computadores. Isto é, sendo os computadores unidades de computação susceptíveis a ataques, os telemóveis também o são, estando por isso sujeitos ao mesmo tipo de ataques e ainda a roubos físicos, sendo assim importante determinar as respostas necessárias para que esta ligação entre o telemóvel e a identidade seja fiável e segura [17].

2.1.3 Segurança dos sistema informáticos

Nos sistemas informáticos é impossível garantir-se uma segurança perfeita. Existirão sempre vulnerabilidades, ataques capazes de os explorar, pessoas dispostas a efectuar ataques e riscos decorrentes desses mesmos ataques. No entanto, a segurança não diz respeito meramente ao que pode falhar, mas sim sobre o que precisa de acontecer de forma correcta. Colocando-se por isso a seguinte questão, até que ponto o investimento em segurança para que a relação custo-benefício seja compensadora [83].

Por exemplo, entidades como a Banca, gerem o seu investimento em segurança com cuidado e atenção, pois é um tipo de negócio em que um dos principais riscos é a reputação da organização.
Ainda assim, é importante que a segurança crie barreiras, vigie procedimentos e limite acções, mas nunca de modo exagerado, pois se interferir excessivamente com a actividade pessoal das pessoas, elas terão tendência a subverter o sistema, contrariando políticas e mecanismos de segurança.

Tendo isto em mente, todas as iniciativas que promovem a segurança junto da sociedade e de acordo com as conveniências da mesma, tanto a nível de sistemas empresariais como governamentais são importantes. Estas serão capazes de reduzir os custos em sistemas de segurança e automaticamente promoverem tanto o comércio como os serviços públicos. Deste modo os sistemas de segurança, baseiam-se essencialmente nas credenciais de identificação e autenticação, sendo vistos de forma muito confiável do ponto de vista da sociedade.
Um exemplo concreto, é a identificação e autenticação diária de milhões de pessoas em computadores, nas entidades bancárias através da Internet, nos aeroportos, fronteiras, entre outros.

2.1.4 Identificação e autenticação electrónica

Dada a rápida convergência das questões de segurança mundial, como o ciber-crime e a ciber-guerra, combinada com as crescentes preocupações em torno da privacidade individual, existe uma necessidade urgente de desenvolver padrões mundiais para auferir a identidade pessoal, em processos de negócios ou governamentais. Como

tal, é necessário que mundialmente sejam adoptadas boas práticas no desenvolvimento e na implementação dos mecanismos de segurança mais apropriados, tendo em conta a privacidade e a segurança de todos [18].

Actualmente os mecanismos de segurança dos métodos de identificação são vulneráveis ao erro humano, à engenharia social e a ataques maliciosos. Cabe assim às organizações calcularem os custos da segurança desejada, tendo sempre em consideração as consequências das medidas tomadas, uma vez que, se estas forem ineficientes ou inadequadas podem resultar em vítimas humanas, custos para as organizações e sobretudo em consequências sociais em termos de segurança e confiança.

Foi desta constatação que surgiram as primeiras movimentações de diferentes países, nomeadamente na adopção de um novo documento de identidade pessoal. Esta decisão consiste primordialmente na implementação de um documento de identificação electrónico capaz de suportar a identidade num formato digital, possibilitando ainda a integração da identidade digital na computação móvel. Pode-se tomar como exemplo o caso particular da Suécia, [49] que integra as características da identidade digital num cartão bancário, possibilitando assim proporcionar e desenvolver novos serviços.

Assim, a característica física mais inovadora do novo documento electrónico é a integração de um chip, isto é, um *smart card*. Este possui um microcomputador embebido, capaz de armazenar toda a informação privada e pública do cidadão, realiza ainda operações criptográficas, e suporta as funcionalidades electrónicas de autenticação e assinatura digital, para além de outras funcionalidades interessantes [10] [58].

Importa referir que a introdução do cartão electrónico, assenta sobretudo nas potencialidades das credenciais de identificação contidas no cartão. Espera-se que estas contribuam significativamente no incentivo à confidencialidade, e à confiança das organizações e dos indivíduos, em todo o mundo. Naturalmente, devido às características internas do *smart card* estas serão capazes de se relacionarem com diversos dispositivos móveis (telemóvel, computadores e outros), promovendo o desenvolvimento de soluções e serviços inovadores, mais concretamente ao nível da camada de segurança [76].

Em suma, é desta perspectiva social, tecnológica e de segurança que surgiu a idealização do projecto *Ticket-ID*, uma vez que o futuro se baseia na utilização do telemóvel enquanto elemento de computação móvel potente e portador da identidade pessoal em constante mobilidade e conectividade. Este facto permitiu perceber as necessidades sentidas na sociedade em termos de termos de segurança em relação a novos serviços e funcionalidades. Assim tendo em conta estes factos e os projectos-piloto um pouco desenvolvidos por todo o mundo, que utilizam as mais recentes tecnologias e o cartão de identidade electrónico, facilmente se constataram as imensas potencialidades e o impacto de confiança na sociedade que estas serão capazes de provocar. Mais precisamente na associação dos mecanismos de privacidade e segurança oferecidos pelo cartão de identificação electrónico ao telemóvel.

2.2 *e-ID* - Identificação electrónica

Actualmente os documentos de identificação pessoais estão a sofrer actualizações um pouco todo o mundo, nomeadamente na transformação do documento convencional de papel para um formato moderno e electrónico à semelhança dos cartões de crédito, vulgo *smart card*.

O sucesso da adesão por parte de diversos países, deve-se sobretudo ao facto de actualmente o *smart card* ser dificilmente penetrável a ataques e a falsificações. Outro factor muito importante é a capacidade que o documento possui enquanto elemento electrónico capaz de se integrar com outros sistemas de computação, permitindo uma maior segurança em termos tecnológicos que antes não existiam.

Estas potencialidades associadas ao cartão revelam que os documentos electrónicos são muito mais seguros, o que vem simplificar o dia-a-dia dos cidadãos e ao mesmo tempo vem reduzir os custos em operações de controlo a fraudes. Consequentemente todas as entidades de segurança e defesa nacional vêm com bons olhos a sua implementação devido à simplificação e à automatização de processos que este proporciona.

2.2.1 Tecnologia associada ao cartão de cidadão

2.2.1.1 Caracterização e potencialidades dos *smart cards*

Como foi frisado anteriormente, o *smart card* contém no seu *chip* electrónico o factor essencial de segurança do documento. Importa assim caracterizar o *chip* e as suas potencialidades.

No caso concreto do cartão de cidadão português, este é produzido pela "Imprensa Nacional-Casa da Moeda"(*INCM*). O conceito do cartão consiste em juntar vários documentos de identificação num único documento (*smart card*), permitindo assim uma máxima interoperabilidade entre várias entidades de acordo com a lei Portuguesa.

O *chip* embutido no cartão pode ser comparado com um microprocessador, tal como um mini-computador com *CPU*. Trata-se dum *Java smart card*.

O *Java Card* neste caso tem um *chip* com um CPU 16/8 bit, a ROM contêm o sistema operativo e os algoritmos de criptografia. Tem a capacidade máxima de 64 KB EEPROM, utiliza a RAM para dados temporários e faz a gestão dinâmica de memória e dos recursos do sistema. É ainda resistente à temperatura e a outro tipo de ataques mais elaborados (manipular e observar a transferência de energia no *chip* do cartão) [58] [10] [47].

O seu funcionamento consiste em responder aos pedidos das aplicações e ao processamento dos dados, mas para isso é necessário um sistema operativo instalado na plataforma de memória do microprocessador. Assim, enquanto *Java smart card* o sistema operativo instalado no cartão executa *Java Applets* via *JCRE(Java Card Run Time Environment)*, este corre no sistema operativo nativo do cartão. O processo que permite estabelecer a comunicação com o sistema operativo é realizado via *APDUS (Application Protocol Data Units)* definidos no standard ISO 7816 [1] [58] [10] [47].

Deste modo, o sistema operativo é o principal elemento que torna seguro o documento, uma vez que é este que define os protocolos de comunicação com o ambiente exterior. Também é responsável por receber, gerir e armazenar a informação na memória do microprocessador, faz o processamento dos dados e as operações criptográficas mais potentes, tais como a criptografia assimétrica através de uma infra-estrutura *PKI*.

Importa ainda referir que existem dois tipos de sistemas operativos: ***os dedicados*** cuja função é correr aplicações especificas; ***os gerais***, que são multi-aplicação podem operar sobre diferentes aplicações (*applets*) [22] [47].

2.2.1.2 Arquitectura - cartão de cidadão

No caso do cartão de cidadão, o sistema operativo do cartão é *geral*, isto é, multi-aplicação, pois contém três *applets* que possibilitam a interacção com o cartão em diferentes aplicações.

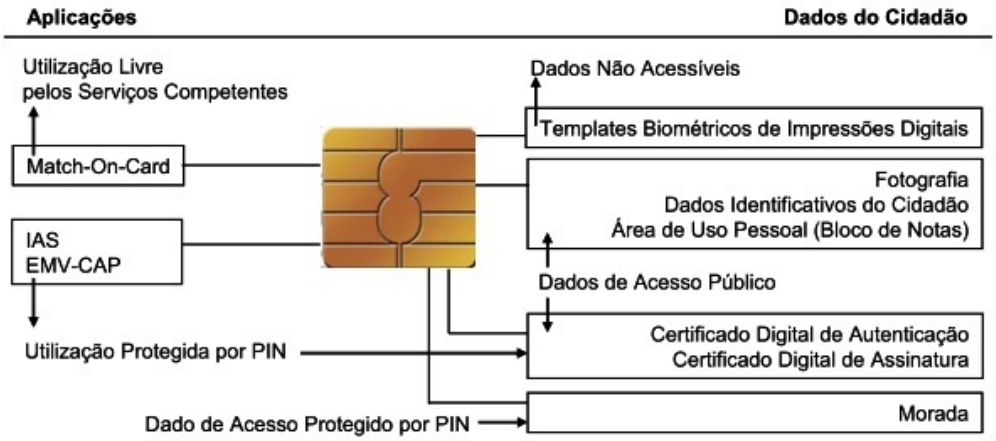

Figura 2.1: *Applets* contidas no *chip* do cartão de cidadão [75].

Dito isto, o cartão de cidadão pode definir-se sendo um documento de identificação electrónico que contém os dados de identificação de cada cidadão e ainda o número de identificação civil, o número de identificação fiscal, o número de utente dos serviços de saúde e o número de identificação da segurança social. Isto possibilita uma maior interacção electrónica junto do Governo Português, nomeadamente no acesso simplificado aos serviços públicos.

Enquanto documento digital, o cartão de cidadão permite ao respectivo titular provar a sua identidade perante terceiros através de autenticação electrónica. O cartão de cidadão permite ainda ao respectivo titular autenticar-se de forma unívoca através de uma assinatura electrónica qualificada que o torna autor de um documento electrónico [75].

A componente electrónica do cartão de cidadão irá permitir ao respectivo titular autenticar-se perante sistemas informáticos e serviços informatizados da administração pública e de entidades privadas, na Internet.

É ainda possível aferir a correspondência entre o portador e o titular do cartão de cidadão através da verificação por via da impressão digital. No *chip* são conservadas as minúcias das impressões digitais do titular do cartão e através duma aplicação é possível comparar as impressões armazenadas no cartão com as impressões recolhidas por um sistema externo de leitura das impressões digitais. Importa referir que a segurança em torno do processo de verificação baseia-se num aparelho apropriado de leitura [6] e no próprio cartão de cidadão. Este dois elementos em conjunto tornam possível fazer a respectiva comparação dentro do próprio *chip* do cartão, *Match-On-Card*, isto é, no decorrer do processo de verificação a informação do cidadão (neste caso as minúcias das impressões digitais) nunca é enviada para análise para uma unidade exterior de computação (computador) [75].

Figura 2.2: Frente do CC português [75].

Figura 2.3: Costas do CC português [75].

2.2.1.3 *Middleware* - cartão de cidadão

A interacção com o sistema operativo do cartão, mais precisamente com as diferentes *applets* contidas no mesmo, possibilitam usufruir das potencialidades acima descritas.

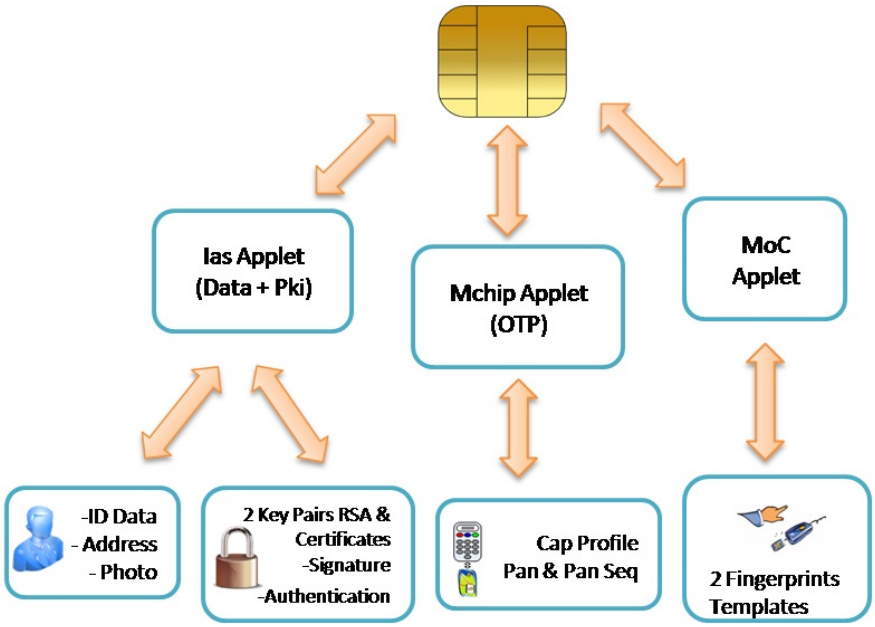

Figura 2.4: Diagrama - *Applets*/*Funcionalidades*.

Como se pode observar no diagrama 2.4, o cidadão tem a possibilidade de usufruir das potencialidades instaladas no cartão através das respectivas *applets* para assim aceder aos dados e à informação relevante. Contudo o acesso não é ilimitado, pois existem partes sensíveis do cartão que estão bloqueadas por um *PIN* pessoal.

Assim, em relação às *applets* apresentam-se as suas respectivas funcionalidades:

- **Ias:** aplicação que permite o acesso aos dados do cidadão e às operações de autenticação e assinatura electrónica.
- **Otp:** aplicação responsável por gerar uma palavra-chave única de forma a ser utilizada em determinados contextos.
- **MoC:** aplicação que armazena o *template* dos dados biométricos do cidadão, permite também a execução do processo de validação dos dados directamente no cartão.

Na prática, a comunicação e o acesso aos dados (informação pública) pode-se realizar utilizando uma aplicação disponibilizada pelo governo português, no site do cartão de cidadão gerido pela *AMA (Agência para a Modernização Administrativa)* [3]. Contudo, esta aplicação disponibilizada pelo Estado Português não possibilita o acesso a todas as *applets* e consequentemente não é possível usufruir de todas as suas funcionalidades.

Além da aplicação disponibilizada também existe um outro método embora mais técnico e apenas recomendável para especialistas da área. Este método consiste em desenvolver um *middleware* que possibilite o acesso aos recursos do cartão, para assim ser possível o desenvolvimento de novas aplicações e serviços. Para tal, é necessário dominar a comunicação ao nível do *smart card*.

Neste contexto, um *middelware* é essencialmente utilizado para mover ou transportar dados entre programas de diferentes protocolos de comunicação, tal como acontece na comunicação entre um *smart card* e um computador. O *middleware* é geralmente constituído por módulos dotados por *APIs* de alto nível que proporcionam a sua integração em aplicações desenvolvidas em diferentes linguagens de programação, e interfaces de baixo nível que permitem a sua independência relativamente ao dispositivo. De um modo muito lato o seu objectivo subsiste em mascarar a heterogeneidade e fornecer um modelo de programação mais produtivo para os programadores [82].

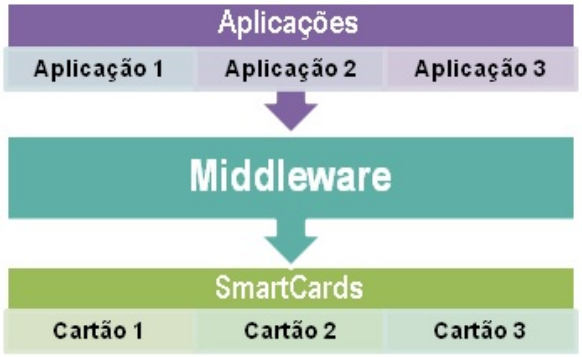

Figura 2.5: Ilustração de um *Middleware*.

Como se pode observar da ilustração 2.5, um utilizador pode usufruir de várias aplicações que comunicam através de um *middleware* com vários cartões. Conforme foi mencionado anteriormente, um *middleware* é um elemento fundamental no processo de comunicação e abstracção entre as aplicações e os cartões.

Dito isto, no caso do cartão de cidadão português também é fornecido pelo Estado um *middleware* capaz de ser integrado em aplicações desenvolvidas por terceiros, mas este não contempla o acesso a todas as funcionalidades e recursos do cartão (faculta apenas as mesmas funcionalidades da aplicação disponibilizada). Contudo, o desenvolvimento de um *middleware* revela-se uma tarefa árdua que requer o domínio de conhecimentos específicos e a interpretação de normas ISO que definem os modelos de comunicação e programação.

Importa ainda referir que o projecto *Ticket-ID* contempla o desenvolvimento de um *middleware* para o cartão de cidadão português, permitindo assim a utilização de vários elementos do cartão na camada de segurança desenvolvida. Ainda assim, o seu desenvolvimento não é simples, pois existem diferentes versões do *chip* do cartão de cidadão e como tal diferentes formas de aceder aos dados armazenados. Sugiram também limitações relativamente à informação técnica existente sobre o cartão de cidadão o que dificulta a forma de comunicar e aceder a determinado tipo de dados.

No capítulo 6 explica-se a metodologia seguida ao longo do processo de construção de um novo *middleware* capaz de comunicar com o cartão de cidadão, esta também pode ser consultada no artigo escrito no âmbito deste projecto [78]. Importa ainda referir que

o desenvolvimento do *middleware* também se relevou útil para outro projecto proposto pela *Multicert*, o qual se baseia numa plataforma que permite auferir a identidade do cidadão no acto eleitoral, contemplado por isso a funcionalidade de MoC (Match-On-Card).

2.2.1.4 STORK - Interoperabilidade dos *e-IDs*

No contexto europeu [19], vários países já aderiram a este novo conceito de identificação, mas o mais importante na utilização dos *smart cards* para além das potencialidades associadas em termos de segurança é a excelente capacidade que estes têm de se integrarem de forma simples na sociedade.

Country	ID Card?	Compulsory (i)/ primary ID	eID Card? (ii)	eID Card Planned?
Austria	yes	no	yes	--
Belgium	yes	yes	yes	--
Bulgaria	yes	yes	(no)	(no)
Cyprus	yes	yes	no	no
Czech Republic	yes	yes	no	no
Denmark	no	--	--	no
Estonia	yes	(yes)	yes	--
Finland	yes	no	yes	--
France	yes	yes	no	yes
Germany	yes	(yes)	no	yes (specs.)
Greece	yes	yes	no	no
Hungary	yes	no	no	yes
Ireland	no	--	--	no
Italy	yes	(yes)	yes (partial)	--
Latvia	no	--	--	yes
Lithuania	yes	yes	no	no
Luxembourg	yes	yes	no	yes
Malta	yes	yes	no	yes
Netherlands	yes	(yes)	yes	--
Poland	yes	yes	no	yes
Portugal	yes	yes	yes	--
Romania	yes	yes	no	yes
Slovakia	yes	yes	no	yes
Slovenia	yes	(yes)	no	yes
Spain	yes	yes	yes	--
Sweden	yes	no	yes	--
UK	yes (partial)	unknown	yes (partial)	--
Iceland	yes	yes	no	yes
Liechtenstein	yes	no	no	yes
Norway	no	--	--	no
Total	25	20	10	13

Figura 2.6: Países com cartão electrónico no 2009 [19].

Dado que num futuro próximo estaremos mais próximos de uma sociedade ubíqua onde tudo estará conectado através da Internet e de dispositivos electrónicos em qualquer lado e em qualquer altura, torna-se importante criar soluções capazes de garantir a segurança e a privacidade pessoal. Tendo em conta este objectivo, os *smart cards* têm uma característica muito especial a elevada capacidade de se integrarem numa plataforma de interoperabilidade de serviços de diferentes países [44].

Um exemplo do desenvolvimento de uma plataforma destas é o projecto STORK [77]. Este é constituído por um consórcio de 29 entidades, incluindo 14 governos e tem como principal objectivo a implementação duma plataforma de interoperabilidade na União Europeia, que possibilite o reconhecimento e a autenticação dos cidadãos através do documento electrónico em qualquer estado membro. Esta plataforma conta também com o desenvolvimento de um *middleware* capaz de comunicar com os cartões dos respectivos países.

O estudo e a análise desta plataforma está ao cargo do *Porvoo Group* [29]. Este grupo tem como objectivos analisar na prática a capacidade desta plataforma partilhar informação entre os diferentes estados membros através da utilização de uma *PKI* e dos *Smart Cards*.

Esta potencialidade pode vir a ser útil no projecto *Ticket-ID*, pois uma plataforma de interoperabilidade permitirá o acesso aos serviços oferecidos pela solução de forma transparente, sem que para isso seja necessário implementar mudanças estruturais no sistema desenvolvido.

2.3 Tecnologias de processamento e comunicação

Esta secção aborda as diversas tecnologias que são utilizadas no projecto *Ticket-ID*. Deste modo, é feita uma descrição num âmbito geral sobre cada tecnologia e depois apresentam-se alguns detalhes técnicos mais interessantes.

2.3.1 *Smart Cards*

2.3.1.1 Enquadramento histórico

Em meados de 1950, o clube *Dinners* implementou o primeiro cartão plástico capaz de efectuar pagamentos sem a intervenção de dinheiro real. Alguns anos mais tarde entre 1968 e 1970, investigadores Germânicos e Japoneses patentearam a ideia de integrar um circuito integrado num cartão de plástico. Mas é em 1974 *Roland Moreno* quem deposita por volta de 50 patentes em 11 países, sendo também nesta mesma altura que aparecem os primeiros cartões com *chips* comercializados pelo grupo francês *CII-Honeywell Bull*, futura empresa *Bull* [63]. A primeira aparição de projectos-piloto com *smart cards* surgiu na França e na Alemanha em meados de 1980, estes projectos abrangiam diversas áreas, tais como: as *comunicações móveis*, onde se utilizava o *Smart card* como cartão um pré-pago capaz de realizar chamadas e as *operações bancárias*, neste caso os cartões eram utilizados como elementos seguros na realização de transacções bancárias (débito/crédito).

O sucesso destes projectos-piloto provaram o potencial desta tecnologia e na década de 1990 as potencialidades associadas a esta tecnologia vieram proporcionar grandes investimentos e novas invenções nos *smart cards* [10].

As mais recentes inovações, permitem incorporar nos cartões elementos de criptografia moderna, o que lhes possibilita a codificação de informações tornando-os mais potentes e seguros. É ainda possível estes armazenarem dinheiro electrónico ou registos médicos pessoais, deste modo a sua inclusão em novas áreas mais críticas, das quais se destacam as telecomunicações, a banca e a segurança, demonstram a sua importância no mundo actual [63].

Assim como se pode constatar a tecnologia sobreviveu, evoluiu e mantém-se em grande destaque nos dias de hoje. Isto deve-se sobretudo aos benefícios associados à tecnologia, nomeadamente, o poder computacional, a portabilidade e a segurança. Sendo a segurança particularmente o elemento mais importante, uma vez que, os benefícios advindos da criptografia permitem criar ambientes onde é possível armazenar e assegurar todo o tipo de informação confidencial (passwords, dinheiro digital, etc). Outra característica muito importante é a dificuldade de copiar os dados do cartão sem o consentimento do seu dono (inserir um código PIN), por oposição aos cartões de fita magnética que são mais facilmente copiados/clonados para fins ilegais.

2.3.1.2 Definição

Um *smart card* pode ser visto como um cartão com um *chip* embutido capaz de armazenar dados e executar comandos. O *chip* é um micro-módulo de área máxima de *25 mm2* colocado, classicamente (não exclusivamente) num cartão de plástico.

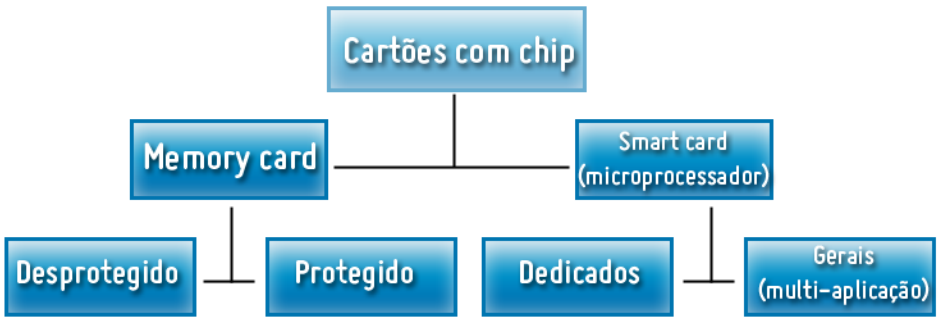

Figura 2.7: Diferentes tipos de cartões.

Como se observa da imagem anterior existem diferentes tipos de cartões e estes dividem-se em duas principais categorias, os cartões de memória (*memory cards*) e os cartões inteligentes com Microprocessador(*Smart Card*).

Os *memory cards*, têm circuitos de memória que permitem o armazenamento de dados. Estes cartões usam uma lógica de segurança baseada em hardware, para controlar o acesso aos dados.

Por sua vez, os *smart cards* dispõem de um microprocessador com uma capacidade limitada de processamento de dados, capazes de realizar a leitura, escrita e processamento dos dados.

Figura 2.8: Ilustração de um cartão com chip.

Importa ainda referir que a concepção e a utilização desta tecnologia deve obedecer aos standards - *ISO/IEC 7816, ISO 7810 e ISO/IEC 14443*.

Desta forma, a norma *ISO 7810*, diz respeito às dimensões, ao formato e aos materiais utilizados na concepção dos cartões de identificação.

No que diz respeito à norma *ISO/IEC 14443*, esta é um standard internacional que define o modo de operação sobre os cartões sem chip, *contactless*. O modo de funcionamento e as potencialidades são algo semelhantes aos cartões com chip, contudo estes baseiam o seu processo de comunicação e de operação a uma distância curta de 10 centímetros do leitor, na frequência de *13.56Mhz*. Também são definidas todas as especificações da transmissão e anti-colisão dos dados.

Finalmente, a norma *ISO/IEC 7816* é a mais conhecida devido à sua importância e é constituída por quinze partes nas quais se especificam as características físicas, os aspectos de segurança e os comandos utilizados para a comunicação entre os *smart cards*(com ou sem *chip*) e outros dispositivos (computadores, leitores, etc...).

2.3.1.3 Protocolos de Comunicação - APDU

A comunicação entre os *smart cards* e outros dispositivos pode ser vista de forma análoga à comunicação realizada entre dois computadores através do protocolo *TCP/IP*, o qual transporta pacotes de dados do emissor para o receptor. No caso dos cartões, estes comunicam utilizando pacotes *APDUS* (Application Protocol Data Units) entre um cartão (*slave*) e um dispositivo (*master*), a definição deste protocolo pode ser encontrada na norma ISO 7816-4 [36].

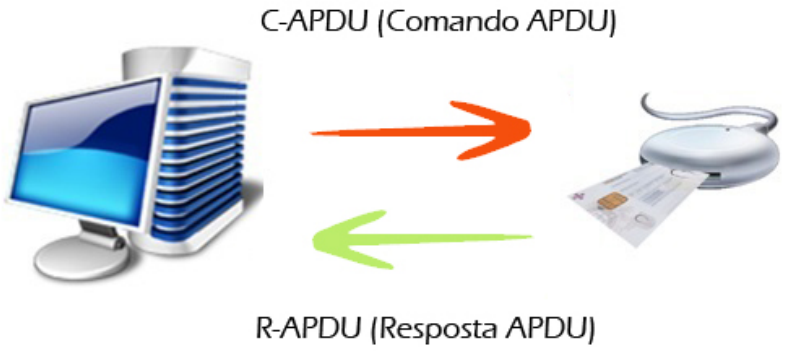

Figura 2.9: *Smart Card* - modelo de comunicação.

Importa ainda referir que a comunicação entre os *smart cards* e um terminal realiza-se no modo *half-duplex*. Isto é, o modelo de comunicação estabelecido é "pedido resposta" de modo a evitar colisões durante o processo de comunicação e isto implica que exista um acordo especifico entre as partes de forma a serem definidos os termos em que se processa a comunicação entre ambas as partes.

Desta forma, o terminal é quem envia sempre os pedidos(*Comando-APDU*) e inicia sempre a comunicação em primeiro lugar(master), o *smart card*(*slave*) tem o papel de receber e processar a respectiva resposta(*Resposta-APDU*) enviando-a no mesmo canal de comunicação.

Este processo de comunicação que resulta numa relação *master-slave* está dependente do funcionamento do sistema operativo contido no *chip* do cartão. Na prática, após o inicio da comunicação o sistema operativo envia um comando *ATR* (*Answer to Reset*) cujo papel é informar acercar do protocolo de transmissão e transferência dos dados suportado pelo *smart card*. Seguidamente coloca-se num estado de adormecido (*low-power* / *sleep mode*) e apenas é activado novamente quando recebe um novo pedido por parte do terminal. Depois de recepcionar o pedido processa a resposta e envia-a, colocando-se imediatamente no estado adormecido à espera do próximo pedido, ver figura 2.10 [58].

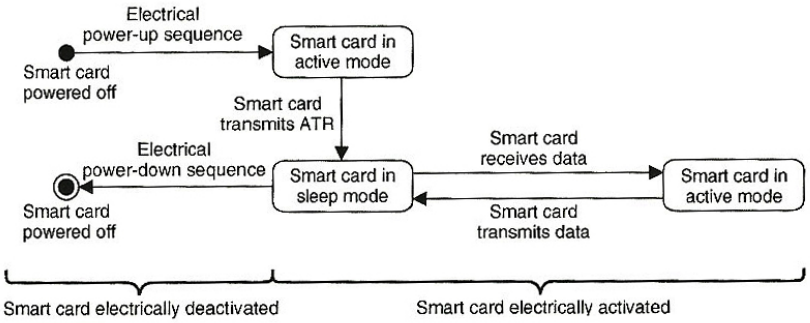

Figura 2.10: Estados da comunicação [58].

O actual cartão de cidadão (*Java Card*) baseia-se neste modelo de programação "pedido-resposta". Contudo, importa referir que é necessário primeiro enviar um comando (*APDU*) para seleccionar a *applet* pretendida (uma vez que existem 3 instaladas no cartão de cidadão português), para seguidamente esta ficar no estado adormecido em espera dos pedidos enviados pelo terminal(*master*).

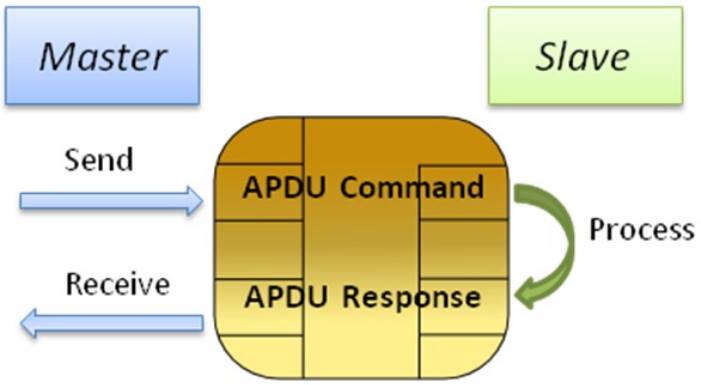

Figura 2.11: Troca de comandos APDUS.

Como se pode constatar qualquer aplicação que comunique com cartões, necessita de implementar este modelo de comunicação com os cartões através do protocolo (*APDU*). Seguidamente, apresenta-se a estrutura dos dois principais comandos *C-APDU* e *R-APDU*.

A estrutura dum comando *APDU*, contem um cabeçalho obrigatório e um corpo opcional:

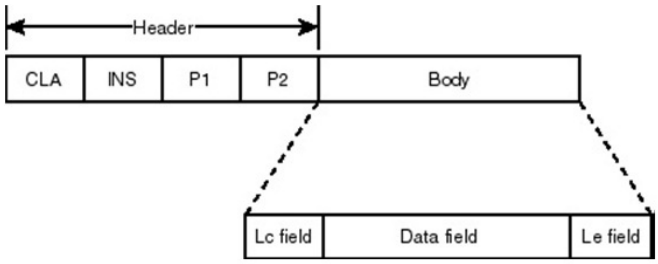

Figura 2.12: Comando APDU.

- **CLA:** *Class Byte* Identifica a classe da instrução
- **INS:** *Instruction Byte* Código da instrução
- **P1 e P2:** Parâmetros utilizados para especificar o *INS*(código de instrução)
- **Le:** Tamanho dos dados devolvidos (bytes).
- **Data:** *Array* de bytes com os dados do comando (opcional).
- **Lc:** Tamanho do *array* de bytes com os dados do comando.

No que diz respeito ao comando de resposta, a estrutura é a seguinte:

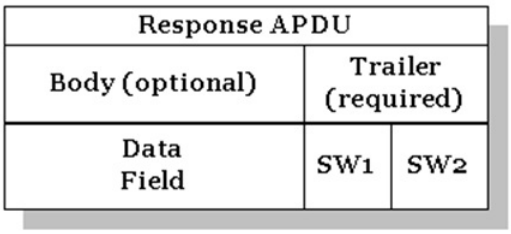

Figura 2.13: Comando de resposta *APDU* [10].

O *APDU* de resposta conta com um corpo opcional, embora dependa do tipo de comando enviado e do sucesso do mesmo. Assim a resposta a enviar pode conter mais dados, neste caso o tamanho destes é definido através do campo *Le* no comando *APDU* enviado. Além do corpo, tem que apresentar sempre dois campos de controlo chamados (*status words - SW*) nos quais consta o respectivo código resultante da execução do pedido.

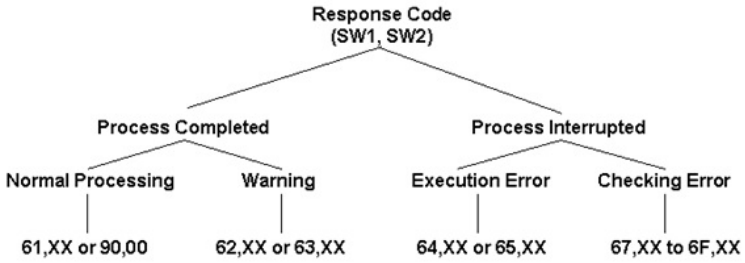

Figura 2.14: Códigos resultantes do *C-APDU* [10].

Os códigos resultantes estão definidos na norma ISO 7816 e o seu significado é fundamental pois representa o feedback devolvido do emissor (cartão) para o receptor (aplicação no computador). Sem este feedback é impossível estabelecer uma correcta comunicação entre ambas as partes.

Importa referir que os códigos resultantes e os dados devolvidos por um *R-APDU* estão em grande parte dependentes do modelo de comunicação, uma vez que a construção de um comando *APDU(C-APDU)*, pode ser feito de quatro formas diferentes:

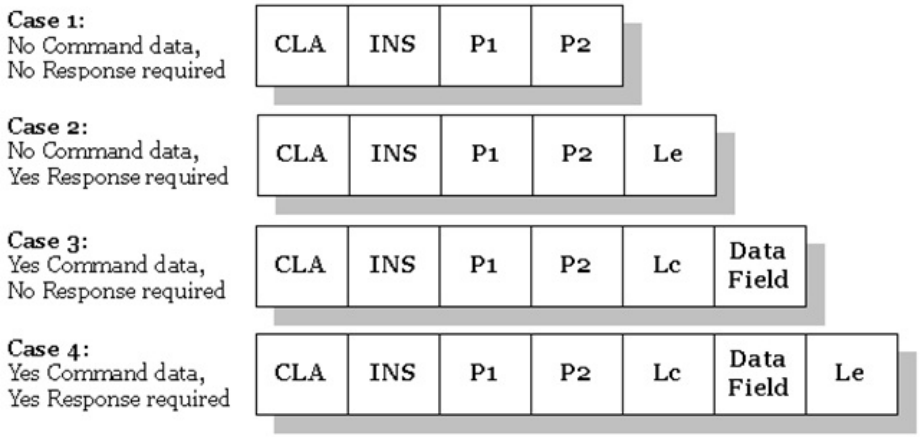

Figura 2.15: Diferentes tipos do Comando *APDU* [10].

No primeiro caso, não são enviados dados para o cartão nem do cartão para o terminal, ou seja, o *C-APDU* contém apenas o cabeçalho e a resposta (*R-APDU*) devolve apenas os dois campos com o código resultante.

No segundo caso, não são enviados dados para o cartão através do *C-APDU*, mas o *R-APDU* retorna dados para o terminal. Isto implica que na construção do *C-APDU* o campo *Le* especifique a quantidade em bytes dos dados devolvidos pelo cartão.

No terceiro caso, já são enviados dados para o cartão através do *C-APDU*, mas não é devolvido qualquer dado do cartão apenas o código resultante. Neste caso o *C-APDU* terá que incluir o campo *Lc*, visto que especifica o tamanho dos dados enviados(bytes) para o cartão.

No quarto caso e último caso, a troca de informação é feita em ambos os sentidos. Assim é necessário que o *C-APDU* inclua os campos *Lc* e *Le*. Por sua vez, a resposta devolvida *R-APDU*, contém os dados enviados pelo cartão bem como o código resultante [10].

2.3.1.4 PC/SC - Interoperability

O *PC/SC* - (*Personal Computer* / *Smart Card*) é uma especificação desenvolvida para facilitar a interoperabilidade e permitir a integração de *Integrated Circuit Card (ICC)*, tecnologia mais conhecida como *smart cards*, no mundo dos computadores. Esta especificação foi projectada para permitir que inúmeras aplicações sejam capazes interpretar os protocolos de comunicação e os métodos de utilização de forma a utilizarem as funcionalidades fornecidas por um ou mais cartões inteligentes de uma forma **flexível**. Deste modo o *PC/SC* baseia-se obviamente na norma ISO 7816, este é compatível com a *Europay-Mastercard-Visa(EMV)* e com o sistema de comunicações móveis(GSM) [12].

O seu contributo é extremamente importante no mundo dos *smart cards*, devido à necessidade de existir um standard que permitisse a interoperabilidade entre diferentes vendedores de cartões ao nível das aplicações que os utilizam. Os benefícios desta tecnologia são inúmeros, mas destacam-se principalmente os reduzidos custos da sua utilização, uma vez que os custos de desenvolvimento e de manutenção das aplicações de um determinado cartão são enormes.

Em suma, todas as aplicações que utilizem a tecnologia standard (*PC/SC*) no processo de comunicação com os *smart cards* trazem imensas vantagens, principalmente às entidades envolventes (produtores, comerciantes, utilizador). Desta forma torna-se possível que que todas as entidades contribuam para o desenvolvimento de novas soluções, proporcionando o sucesso da tecnologia.

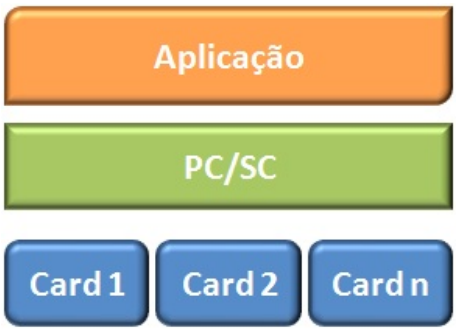

Figura 2.16: Ilustração do standard *PC/SC*.

Um exemplo prático da utilização deste standard no processo de comunicação entre o cartão e uma aplicação é o caso do cartão de cidadão. Tal como se referiu anteriormente o *middleware* disponibilizado com o cartão de cidadão, faz uso do standard *PC/SC* o que permite que os utilizadores tenham acesso e possam manipular a informação pública disponibilizada pelo cartão, sem que para isso seja necessário recorrer a tecnologia especifica e complexa de usar pelos utilizadores/programadores.

2.3.2 RFID - *Radio Frequency IDentification*

Nesta secção aborda-se a tecnologia RFID dado que os *smart cards* sem *chip* (*contactless*), como se referiu anteriormente e na maioria dos casos baseiam o seu processo de comunicação e de operação a uma curta distância do leitor.

2.3.2.1 Enquadramento

A tecnologia RFID surgiu na época da Segunda Guerra Mundial tendo sido utilizada nos sistemas de radares o que motivou a sua popularidade na aviação, nos sistemas de identificação (amigo/inimigo). Contudo ao longo dos anos até aos dias de hoje, esta tecnologia pode ser vista em diversas áreas, não só na identificação, mas também em áreas como a identificação de objectos, monitorização das condições de um objecto, segurança, vigilância, exemplos constatados de grande sucesso tem-se a indústria, veículos, automatização, animais e outros. O crescente desta tecnologia deve-se em muito aos fortes investimentos feitos na microelectrónica, organizações, universidades, e em laboratórios governamentais [72] [40].

O RFID é tido como a Internet das coisas. Esta expressão tenta descrever o número de tecnologias e de projectos de investigação que permitem ter um enorme número de etiquetas inteligentes a interagir com a transmissão de informações entre si e com os sistemas centrais e descentralizados. Pode-se imaginar um conjunto diversificado de objectos físicos do mundo real que são identificados por RFID e onde cada um tem uma presença digital fundamental [11].

2.3.2.2 O sistema RFID

O sistema RFID é constituído normalmente em três partes:

- Estação Base (Leitor): Sistema que realiza as comunicações com a *tag*.
- *Tag* : Pequeno circuito embebido de comunicação, pode-se encontrar em *smart cards*, *smart labels*, e outros.
- Sistema de Informação: base dados que contém a informação a ser processada.

Dependo das aplicações pretendidas e da frequência aplicada, as RFID *tags* podem ser categorizadas em passivas e activas. O *modo activo*, utiliza baterias internas e permite comunicar a distâncias superiores. Por sua vez, *modo passivo* não utiliza qualquer tipo de baterias, uma vez que, na prática ele opera devido à energia vinda do sinal da estação base. Como consequência a distância de comunicação é muito pequena [62] [21].

Um dos problemas que se levantou ao longo do tempo foi o custo desta tecnologia, mas após o forte investimento e o estudo desenvolvido nesta área, hoje em dia existem diversos tipos de *tags* bastante eficazes e desenvolvidas a um custo muito reduzidos.

A tecnologia é composta no seu núcleo por um conjunto de números. Cada *chip* possui um código electrónico de produto que é único (também conhecido como *EPC - Electronic Product Code*) que é acedido por meio de antenas de radiofrequência. Assim, podem ter-se etiquetas coladas em quaisquer tipos de objectos ou pessoas, animais, e quando se dá o contacto entre a *tag* e o leitor, é transmitida a informação por antenas com frequência compatível e essas antenas activam o *chip*, electronicamente, identificando o produto [62].

Figura 2.17: Tags RFID.

2.3.2.3 Aplicações da tecnologia RFID

Uma das aplicações muito conhecida do RFID é o controlo de stocks, deste modo a solicitação para reposição imediata do produto vendido é feita automaticamente reduzindo-se assim os custos operacionais de gestão de stocks. Outra utilidade dada às etiquetas RFID é a prevenção de roubos em lojas e supermercados. Além destes exemplos existem muitos outros pois assiste-se actualmente a uma massificação da utilização do RFID um pouco em todas as áreas, o que contribui definitivamente para a sociedade ubíqua.

Contudo também existem algumas preocupações associadas a esta tecnologia. A privacidade é uma das principais visto que existe a possibilidade das *tags* serem lidas sem o consentimento do proprietário. Sendo que esta preocupação aumenta significativamente no caso das *tags* transportarem informação privada. Outra sensibilidade que apresenta é a diminuta dimensão das *tags* pois podem ser colocadas em locais ou cidadãos sem o seu consentimento.

Como qualquer outra tecnologia existem preocupações inerentes para as quais é necessário encontrar soluções capazes de garantirem que a tecnologia é uma mais valia para a sociedade. A implementação e o sucesso desta tecnologia deve-se em grande parte a várias entidades e organismos que encontraram soluções associadas à criptografia, tais como: *Kill Switches*, *Anonymous Authentication* [14], *Blocker Tags* [37], *Stick-Tags* [7], entre outras capazes de garantirem da forma mais segura a implementação da tecnologia [72] [5] [42].

2.3.2.4 RFID - Cartões de proximidade

Tal como foi referido anteriormente na secção dos *smart cards*, actualmente existem cartões sem *chip* (proximidade) que baseiam o seu funcionamento e a sua concepção na tecnologia RFID. Importa referir que a criptografia e os mecanismos associados permitiram em grande parte o sucesso dos cartões sem *chip* na sociedade. Exemplo concreto deste sucesso é o metro de Lisboa que utiliza cartões sem *chip* como forma de transporte e pagamento dos bilhetes *http://www.otlis.com.pt/*.

Um outro exemplo é cartão de crédito (EMV) de proximidade que será utilizado num futuro próximo. Este recebe energia do terminal e seguidamente o processador transmite as informações para o terminal na frequência de 13,56 MHz. Essa frequência foi escolhida pela sua adequação ao acoplamento indutivo, resistência à interferência ambiental e baixa taxa de absorção pelos tecidos humanos. Os conjuntos de instruções embutidas no processador cifram os dados durante a transmissão.

Sempre que cartões de crédito estão envolvidos, as pessoas preocupam-se com a segurança. Enviar os dados do cartão de crédito para um terminal através de um sinal de rádio poderia ser visto como algo pouco seguro, mas quando o processo funciona correctamente, na verdade é mais seguro do que usar um cartão de crédito de banda magnética.

É neste contexto que surge o *MiFare*, um *standard open-source* (criado pela *Philips* regulamentado pela *NXP Semiconductors*) que lidera a indústria dos *smart cards contactless*. Este standard define o protocolo de codificação e autenticação no decorrer de uma comunicação, de acordo com as especificações do ISO/IEC 14443A.
Existem diferentes cartões no mercado, mas são abordados em especial os *MiFare Classic*, figura 2.18, e em concreto o modelo *MF1 IC S50* (MiFare 1kb). Este cartão *MiFare Classic* consiste num cartão de plástico com as medidas especificadas pelo *ISO/IEC 7810* de tipo ID-1, com uma antena e com um *chip* embebidos. O *chip* é constituído pela interface RF (Rádio Frequência), pela unidade de controlo digital e pela memória(*EEPROM*). Os dados e a energia são transferidos via *RF* pela antena [64].

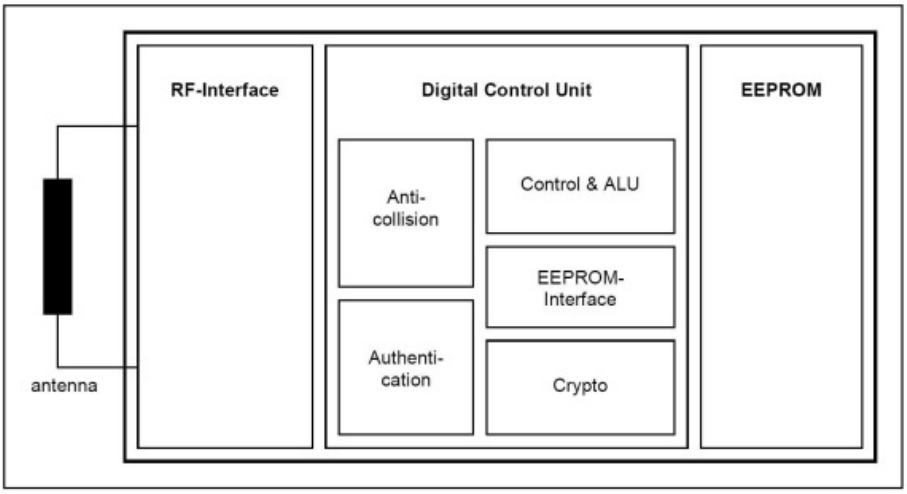

Figura 2.18: Cartão *MiFare Classic* [64].

A figura seguinte apresenta a organização da memória do cartão *MiFare Classic* que tem *1kbyte* de memória *EEPROM*. Esta organiza-se em 16 sectores com 4 blocos e cada bloco é constituído por 16 bytes.

		Byte Number within a Block														
Sector	**Block**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	**Description**
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

Figura 2.19: *EEPROM MiFare Classic* - 1kb [64].

Como se pode observar da imagem 2.19 que ilustra a memória do cartão, existem três tipos diferentes de blocos que armazenam a informação: O primeiro, *Manufacturer Block*, é o primeiro bloco do primeiro sector e contem os dados do fabricante. Quando é produzido é programado pelo fabricante, ficando este bloco protegido contra escrita. Já os primeiros quatro bytes do bloco contem o número de serie.

O segundo bloco, *Sector Trailer*, contem as chaves secretas A e B do sector e as condições de acesso para todos os blocos desse sector, os bits de acesso também especificam o tipo de acesso(leitura, escrita ou valor) dos blocos de dados.

O terceiro e último, *Data Blocks*, são utilizados para armazenar informação privada. Os blocos de dados podem configurar-se para o modo de leitura, escrita ou de valor. No caso de valor estes modo é utilizado em principalmente em aplicações onde operações aritméticas são efectuadas sobre os valores armazenados.

No que diz respeito, ao modo de comunicação como foi referido anteriormente os cartões de proximidade baseiam-se no *ISO7816* e consequentemente o acesso a aplicações via computador, normalmente utiliza o standard *PC/SC* para estabelecer a comunicação entre ambas as partes [2].

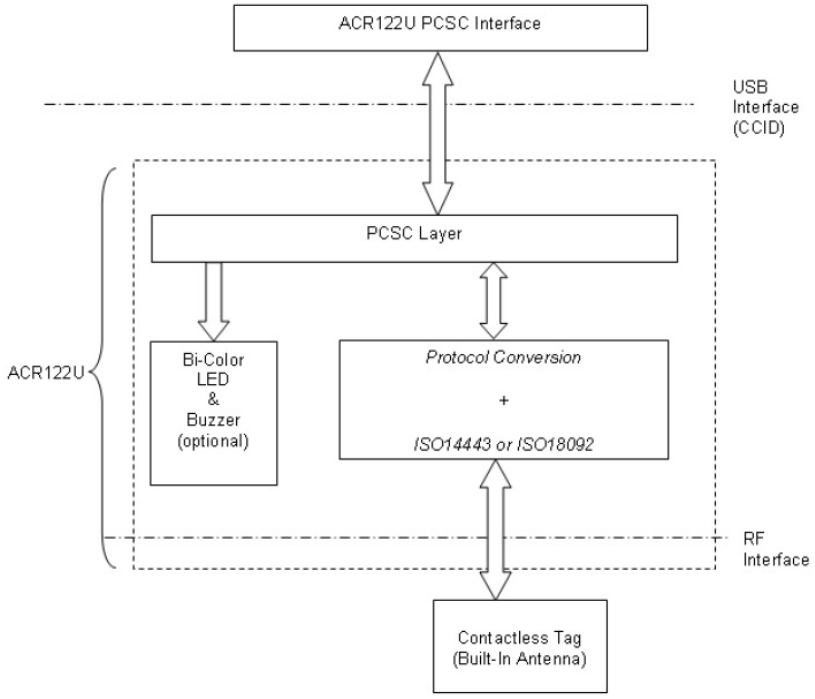

Figura 2.20: Modelo de comunicação dos cartões *MiFare* [2].

A imagem 2.20 refere-se ao esquema de comunicação do leitor contactless(NFC) *ACR122u*, mas o importante a reter deste modelo de comunicação é importância da norma standard *PC/SC* nos cartões *contactless*.

2.3.3 NFC - *Near Field Communication*

O *Near Field Communication(NFC)* é a tecnologia mais recente que permite a comunicação sem fios. Esta foi desenvolvida a partir da combinação de tecnologias de proximidade (RFID) e de identificação existentes.

2.3.3.1 Enquadramento

O NFC resultou de um importante esforço da *Royal Philips Electronics* e da *Sony Corporation*. Em 2004 estas empresas formaram o *NFC Fórum* com o intuito de promover a implementação desta tecnologia junto da sociedade. Contudo para alcançar esta meta foi necessário definir um standard da tecnologia NFC capaz de garantir a interoperabilidade entre dispositivos e serviços, dado que outras tecnologias não tiveram sucesso no passado devido à falta de interoperabilidade entre dispositivos e tecnologias.

2.3.3.2 O sistema NFC

A tecnologia NFC assemelha-se à tecnologia RFID, devido à sua concepção electrónica e às funcionalidades disponíveis de alcançar através de vários dispositivos electrónicos, tais como os telemóveis, *smart cards* e outros. Os dispositivos equipados com a tecnologia NFC utilizam uma *tag* identificadora que tem o papel de assegurar as capacidades de escrita e leitura.

Tal como o RFID, o NFC também foi projectado para comunicações de curta distância neste caso 20 centímetros apesar de tipicamente ser usado a menos de 10cm. Opera globalmente na frequência de banda de 13.56Mhz e suporta a transferência de dados entre dispositivos nas velocidades de 106kbps, 212kbps e 424kbps [54].

Quando se estabelece uma comunicação, esta pode ser realizada de dois modos diferentes(tal como o RFID):

- *Modo activo:* os dois dispositivos que comunicam tem que estar activos, isto é, têm de gerar os seus próprios campos de rádio frequência para enviar dados, sendo que o campo de RF é alternadamente gerado por cada dispositivo.
- *Modo passivo:* neste modo, a comunicação ocorre entre um dispositivo activo (terminal de leitura) e um dispositivo passivo(*Smart Card*), sendo que o dispositivo passivo não tem bateria e usa o campo de RF gerado pelo dispositivo activo para enviar dados.

No que diz respeito, aos standards da tecnologia NFC, esta é compatível com os actuais standards *contactless* e suporta ainda dois protocolos próprios, o NFCIP-1 que está definido no ISO18092, ECMA340 e ETSI TS 102 190, e o NFCIP-2 definido na ISO21481, ECMA352 e ETSI TS 102 312. Estes standards definem as características básicas, nomeadamente os esquemas de codificação e modulação dos bits (Manchester e Miller) e ainda as velocidades de transferência, os protocolos de transporte da informação e os modelos anti-colisão durante a comunicação [54].

O protocolo NFCIP-2 permite seleccionar um destes três modos de operação [71]:

- *Modo Leitura/Escrita*: o dispositivo NFC é capaz de ler dados de etiquetas NFC.
- *Modo Peer-to-Peer*: dois dispositivos NFC podem trocar dados. Por exemplo, a troca de contactos pessoais entre telemóveis.
- *Modo Emulação de Cartões*: o próprio dispositivo NFC comporta-se como sendo uma etiqueta NFC, fazendo-se passar por um *smart card contactless* (ISO14443) perante um leitor.

2.3.3.3 Aplicações da tecnologia NFC

Assim, o NFC pode ser utilizado num vasto leque de aplicações, tal como transferir e sincronizar informações entre dispositivos, sendo que um dos grandes objectivos desta tecnologia é simplificar alguns processos do dia-a-dia. Exemplos destes processos são os pagamentos através de dinheiro digital, compra de bilhetes através do telemóvel e os sistemas de fidelização armazenados no telemóvel [38].

A interligação da tecnologia NFC com os telemóveis proporciona o aparecimento de novas oportunidades de negócio tendo em conta, a segurança e a rapidez desejada, dado que a maioria das pessoas possui telemóvel e esta receptiva a novas soluções nesta área.

A imagem seguinte 2.21 ilustra a arquitectura proposta pela *GSM Association* como modelo de comunicação para o acesso a serviços através de telemóveis NFC [30].

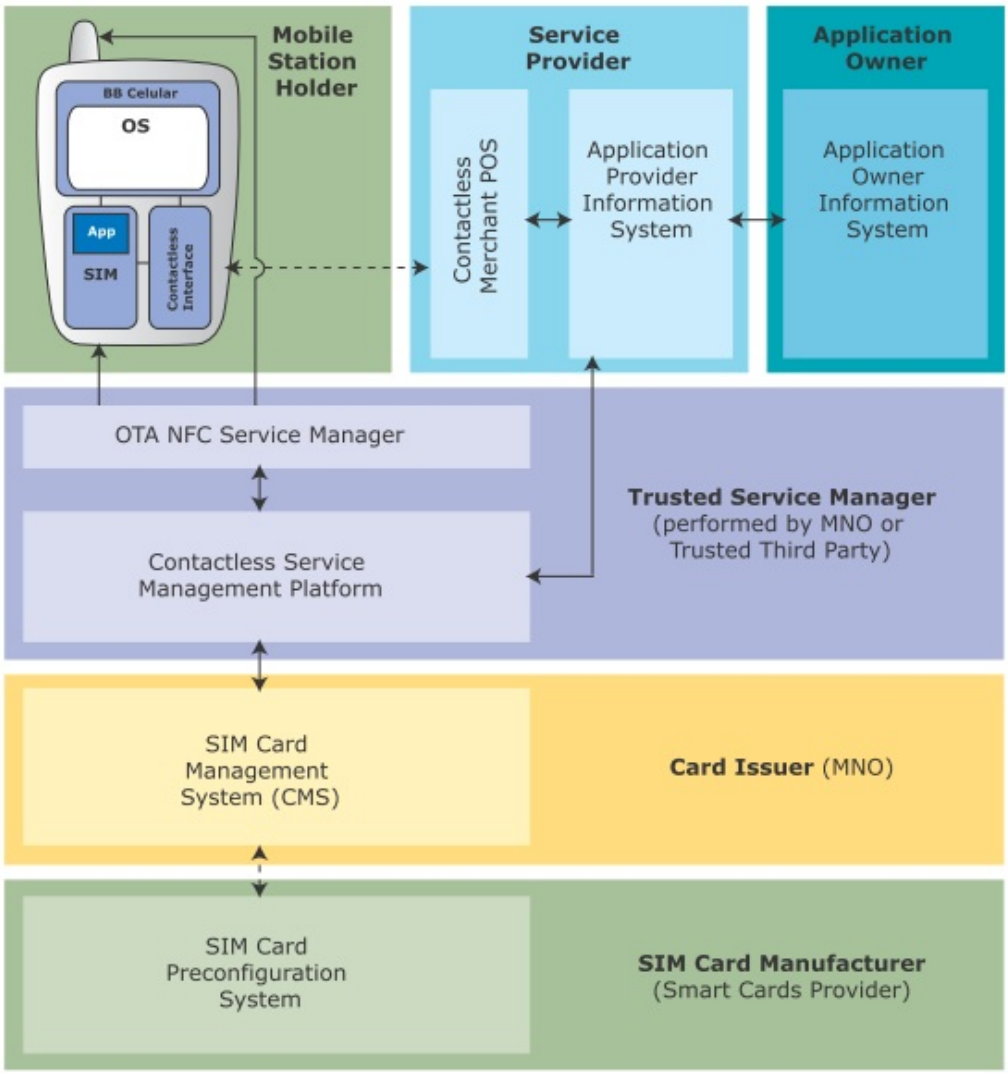

Figura 2.21: Modelo de comunicação NFC em telemóveis [30].

2.3.3.4 Perspectiva do projecto - Tecnologia NFC

Torna-se ainda importante referir que estas duas tecnologias, RFID e NFC, foram abordadas neste documento com o objectivo de investigar o modo de funcionamento destas novas tecnologias e as potencialidades associadas as mesmas, com o intuito de serem integradas no projecto *Ticket-ID*, nomeadamente na sua associação através do *telemóvel* ou de *smart cards contactless* como portadores de bilhetes.

Como será abordado mais adiante a utilização da tecnologia NFC deve-se aos inúmeros projectos-piloto na área da bilhética associados a esta tecnologia, e ainda pelas inúmeras vantagens desta tecnologia em relação a outras (Bluetooth, IrDa, RFID). Exemplos destas vantagens são a rapidez no processo de comunicação, os três modos de comunicação possíveis, os custos reduzidos e a capacidade de funcionar com as infra-estruturas já existentes (RFID), para além de possibilitar a troca de maiores quantidades de informação ao longo da comunicação em comparação com o RFID.

Contudo, antes de se implementar qualquer tecnologia que seja utilizada por um grande número de pessoas é necessário perceber as suas vulnerabilidades e neste caso torna-se importante perceber mais concretamente os possíveis ataques a que está sujeita a sua implementação nos telemóveis, uma vez que actualmente os telemóveis são vistos como grandes dispositivos de computação móvel.

Deste modo, importa referir que após uma análise geral, os principais receios baseiam-se em ataques: *EavesDropping*, *Data Modification* e *Man-In-The-Middle* [48] [13]. Por outro lado o furto do telemóvel também é preocupante pois o atacante poderá utilizar o telemóvel para aceder a todos os serviços activos, tais como os bilhetes de transportes públicos, entre outros que não requerem uma autenticação específica.

2.3.4 A Tecnologia de Código de Barras

A tecnologia do código de barras (1D) é das mais usadas a nível mundial para a identificação de produtos ou objectos. Esta tecnologia consiste na representação gráfica da informação por meio de linhas verticais. No que diz respeito à informação armazenada, este tipo de código de barras, apenas suporta a codificação numérica, já o

seu aspecto gráfico pode variar consoante o *standard* utilizado. O seu sucesso deve-se em grande parte aos baixos custos de implementação e à simplicidade de utilização por meios humanos e informáticos.

2.3.4.1 Enquadramento

O código de barras existe à aproximadamente 40 anos e esta tecnologia consiste em armazenar informação sobre a forma de imagem, mais precisamente barras verticais pretas, que são lidas através de um leitor detector de foto células que detecta o código de barras quando a luz que emite for reflectida para si. Esta luz é posteriormente convertida para um sinal eléctrico e por último identificado o conjunto de números que representa a informação que o código de barras armazena.

Na leitura dos códigos de barras 1D, considera-se somente a largura das barras e o seu espaçamento. A altura das barras apenas representa a redundância dada ao símbolo e por isso estes códigos apenas são lidos numa dimensão [50]. Outro aspecto importante é o facto da informação lida não conter mais do que uma dúzia de números, por isso o código de barras, na sua esmagadora maioria dos casos, não passa de um registo numa base de dados a partir do qual é possível obter mais informações sobre o produto em questão. Existe um conjunto vasto de exemplos, mas talvez o mais óbvio e ilustrativo é o caso do supermercado, isto é, quando os produtos são passados pela caixa registadora é possível obter a informação relativa a cada produto.

Nesta secção, aborda-se a nova geração do código de barras, mais precisamente os códigos de barras bidimensionais (2D) uma vez que estes têm mais potencialidades e são cada vez mais utilizados em diversas áreas de forma inovadora.

2.3.4.2 A tecnologia *QR-Code*

Os códigos de barras 2D devem ser vistos como a evolução do código de barras 1D. Esta nova forma de armazenar informação permite guardar grandes quantidades de informação visto que os dados são codificados tanto em largura como em altura originando uma forma quadrada e por isso a quantidade de informação contida num único símbolo (código) é muitíssima maior do que em símbolos unidimensionais. Como se pode constatar este tipo de codificação apresenta muitas vantagens, destacando-se a

elevada capacidade de armazenamento pois é possível guardar mais de 4000 caracteres alfanuméricos ou 7000 numéricos numa única imagem. Desta forma um produto contém no seu código de barras mais informação e assim não existe uma necessidade de ter acesso a uma base de dados.

A codificação dos códigos de barras 2D é bidimensional e visualmente assemelha-se a um quadrado, os algoritmos de codificação mais usados são: *QR Code, Aztec, Datamatrix, Maxicode, Micro PDF417, PDF 417,* entre outros. Neste caso, vamos abordar em particular o *QR Code*, pois muito provavelmente é o algoritmo mais utilizado (principalmente no Japão) e o mais difundido em todo o mundo.

O *QR-Code (Quick Response Code)* foi desenvolvido pela empresa Japonesa *Denso Wave Corporation* em 1994. Consiste numa matriz 2D composta por um conjunto de pontos pretos e brancos ao longo do *eixo-x* e do *eixo-y* que no seu todo contêm a informação codificada. O seu aspecto visual como se pode constatar pela imagem seguinte, apresenta características especiais como os quadrados nos cantos da imagem, estes permitem identificar a direcção da imagem e reconhecer a imagem como um padrão *QR-Code*.

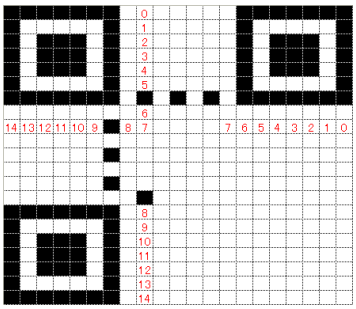

Figura 2.22: Código de barras 2D - Padrão*QR-Code* [70].

No que diz respeito ao processo de codificação, este está definido na norma ISO/IEC 18004. Ainda assim a estrutura do *QR-Code* é bastante simples de visualizar. Como mostra a figura seguinte 2.23 , os 3 quadrados principais definem o padrão, o espaço a azul contem informação acerca do formato da informação e o espaço amarelo é onde esta codificada a informação [70].

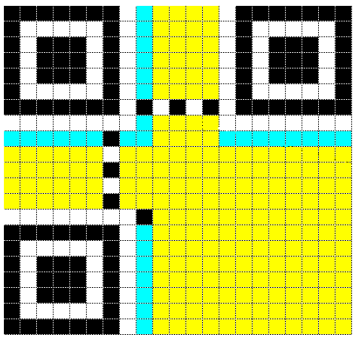

Figura 2.23: Código de barras 2D - Codificação *QR-Code* [70].

Em termos de comparação com o código de barras 1D a codificação apesar de ser mais complexa é muito mais vantajosa e veja-se que no *QR-Code* é possível armazenar maiores quantidades de informação e em dimensões muito mais reduzidas e é ainda resistente a degradações do símbolo e é capaz de ser lido a 360 graus por qualquer leitor. Sendo que uma grande vantagem é o facto do leitor não necessitar de ser um modelo especifico capaz de ler código de barras 2D, pois qualquer câmara Web ou a simples câmara de um telemóvel é capaz de descodificar instantaneamente o símbolo (desde que possua o descodificador correcto). Além destas vantagens facilmente visualizáveis, importa ainda referir que em muitas aplicações codifica-se um simples URL dentro do código de barras o que possibilita apontar para outro tipo de informação.

2.3.4.3 Aplicações da tecnologia de Código Barras 2D

Os códigos de barras 2D têm vindo a ser usados cada vez em mais áreas, sobretudo naquelas onde através dos telemóveis é possível obter mais informações sobre os produtos. A elevada capacidade de armazenar e ler códigos de barras a partir do telemóvel tornou-se um uso global e praticamente acessível a qualquer pessoa.

Após realizada uma pesquisa mais detalhada sobre as potencialidades e os sistemas que utilizam actualmente esta tecnologia, encontram-se algumas aplicações bastantes interessantes. Apresentam-se alguns casos de sucesso [16] [73]:

- *Bilhete electrónico* - Actualmente algumas entidades codificam os bilhetes para determinados eventos recorrendo a esta tecnologia, assim o processo de validação dos mesmos é possível de ser realizado através do ecrã do telemóvel.

- *Anúncios publicitários* - É possível criar novas formas de publicidade através de códigos de barras colocados em *outdoors*, *t-shirts*, cartões de visita, cupões, etc.

- *Conteúdo informativo* - No Japão é tão generalizado o uso do *QR-Code* que até os túmulos já permitem aceder à informação acerca do falecido. Em Paris, é possível encontrar nas paragens dos autocarros códigos com informações sobre os horários e as rotas. Também no museu de Viena, determinadas obras tem um código associado que permitem aos turistas obterem mais informações.

- *Esteganografia* - Existem também algumas propostas interessantes que utilizam o *QR-Code* para esconder informações confidenciais [9].

- *Realidade Aumentada* - Na aérea da realidade aumentada também se podem encontrar algumas aplicações onde é possível associar o código de barras e visualizar num computador (captura da imagem a partir de uma câmara web) uma imagem projectada pelo *QR-Code*. Isto possibilitará num futuro próximo, por exemplo, obter a imagem de um produto que se encontra fechado na sua caixa original através da sua representação virtual [39].

2.3.4.4 Perspectiva do projecto - Integração da tecnologia *Qr-Code*

Actualmente os códigos de barras 2D já são utilizados na área da bilhética, tal como acontece nos jogos do *Sport Lisboa e Benfica* onde é possível através da Internet comprar o bilhete e receber o mesmo via uma MMS no telemóvel, sendo posteriormente validado no estádio por um leitor capaz de ler os respectivos bilhetes através do ecrã do telemóvel.

Tendo em conta as potencialidades desta tecnologia decidiu-se integrar a mesma na arquitectura da plataforma desenvolvida. Isto deve-se ao facto de actualmente não serem ainda comercializados telemóveis com a tecnologia NFC, o que deste modo possibilita criar uma alternativa viável capaz de armazenar as informações pretendidas e outras (URL com o comprovativo do bilhete adquirido). Desta forma o bilhete também ganha características mais reais do que simplesmente caracteres guardados num formato binário na memória do telemóvel.

Por outro lado, o *QR-Code* apresenta-se como uma alternativa a todos os *players*(comerciante, consumidor), isto é, qualquer pessoa tem a possibilidade de escolher a tecnologia que pretende utilizar, já do ponto de vista dos comerciantes estes também podem optar ou até possuírem os dois tipos de sistemas. No caso concreto dos comerciantes, esta tecnologia talvez seja mais convidativa pois a sua inclusão na sociedade é mais antiga e os custos associados à mesma também são mais reduzidos.

Figura 2.24: Ilustração de um bilhete no formato 2D.

2.3.5 Resultados

Esta secção apresenta algumas considerações sobre as tecnologias de processamento, armazenamento e comunicação abordadas ao longo da investigação realizada com o objectivo de serem integradas no projecto *Ticket-ID*.

Deste modo, desenvolveu-se a tabela (2.1) a qual resume as potencialidades de cada uma das tecnologias de acordo com os termos definidos e segundo os critérios, *Baixo - Médio - Alto* com o objectivo de construir uma base comparativa entre as tecnologias.

	QR-Code(2D)	RFID	NFC	Smart Card
Tecnologia	Armazenamento	Comunicação	Comunicação	Comunicação Armazenamento
Custo de implementação	Baixo	Médio	Alto	Médio
Desempenho da comunicação	Médio	Alto	Alto	Médio
Durabilidade	Média	Média	Alta	Alta
Simplicidade de utilização	Alta	Alta	Média	Média
Quantidade de informação	Média	Baixa	Média	Alta
Qualidade da informação	Média	Média	Alta	Alta
Rapidez de processamento	Alta	Alta	Média	Média
Segurança dados	Baixa	Média	Alta	Alta
Interoperabilidade	Alta	Média	Média	Média
Resiliente a ataques	Baixo	Baixo	Médio	Médio

Tabela 2.1: Análise comparativa das tecnologias.

Realizando-se uma breve análise através da tabela, no caso do *QR-Code* esta tecnologia tem como principais vantagens os custos, a rapidez, a simplicidade e ainda a capacidade de ser englobada com outras tecnologias. Estas características tornam o sistema consistente do ponto de vista da usabilidade, contudo em termos de segurança o sistema demonstra algumas fragilidades.

O RFID por sua vez, equipara-se em parte ao *QR-Code* apesar de em termos de segurança dos dados ser mais sólido, no entanto os custos de implementação são mais elevados e a quantidade de informação possível de armazenar é mínima, o que implica mais investimento em sistemas de informação adicionais.

No caso do NFC e dos *Smart Cards*, ambas as tecnologias são bastante uniformes em termos de vantagens e potencialidades associadas a cada uma respectivamente. Ainda assim o NFC acrescenta a capacidade de estar associado a um telemóvel o que possibilita a comunicação remota com outros sistemas, sendo por isso mais abrangente.

2.3.6 Conclusões

Como se pode constatar, todas as tecnologias aqui referidas são actualmente as mais utilizadas a nível mundial em diversas áreas, mas sobretudo na área da bilhética. Exemplo disso são os *smart cards*, RFID e o Código de Barras, outras como o caso particular do NFC apresenta-se ainda numa fase de implementação na sociedade onde os mais recentes projectos-piloto demonstram ser viáveis e sustentáveis na sua inclusão na sociedade.

Ainda assim, o objectivo primordial deste capítulo depreende-se pelo facto de se desenvolver um sistema inovador capaz de aproveitar as melhores características de todas estas tecnologias de forma a obter-se um novo sistema que deve ser visto como um todo. Este deve ser viável do ponto de vista do ciclo de vida de um bilhete, sendo que aqui as tecnologias utilizadas têm um papel fundamental no sucesso do sistema. Por sua vez, o sistema também deve ser seguro e para isso deve possuir todos os mecanismos de segurança que do ponto de vista do cidadão sejam capazes de assegurar de forma simples a sua integridade.

Importa mais uma vez referir que embora seja apresentado um sistema inovador projectado minuciosamente em todas as vertentes, o sistema não pretende ser um concorrente dos sistema desenvolvidos por grandes organizações, mas sim apresentar-se como um sistema íntegro capaz de apresentar na sua camada de segurança elementos que possibilitem a associação da identidade pessoal a valores/objectos (bilhete) intangíveis.

Capítulo 3

Estudo e análise de sistemas de pagamentos

O presente capítulo apresenta um estudo detalhado sobre os actuais sistemas de pagamento de serviços relacionados com a utilização dos telemóveis. Pretende-se analisar e comparar as soluções existentes.

3.1 Análise dos sistemas de pagamento

A área da bilhética é constituída por diversas entidades, nomeadamente os comerciantes, os bancos e o consumidor que no seu conjunto formam o ciclo de vida de um bilhete. Actualmente com o surgimento das novas tecnologias surgiram também novos intervenientes, nomeadamente as operadoras de redes móveis, interessadas em fazer parte do sistema de pagamentos.

Este interesse é muito devido à importância que o telemóvel representa para a sociedade mundial, dado que as potencialidades que lhe estão associadas evoluem constantemente. Como tal, a inserção de um novo serviço no telemóvel que possibilite aos cidadãos adquirir serviços e pagar os mesmos utilizando simplesmente o seu telemóvel, é visto pelas operadoras e pelos fabricantes de equipamentos como uma oportunidade de negócio.

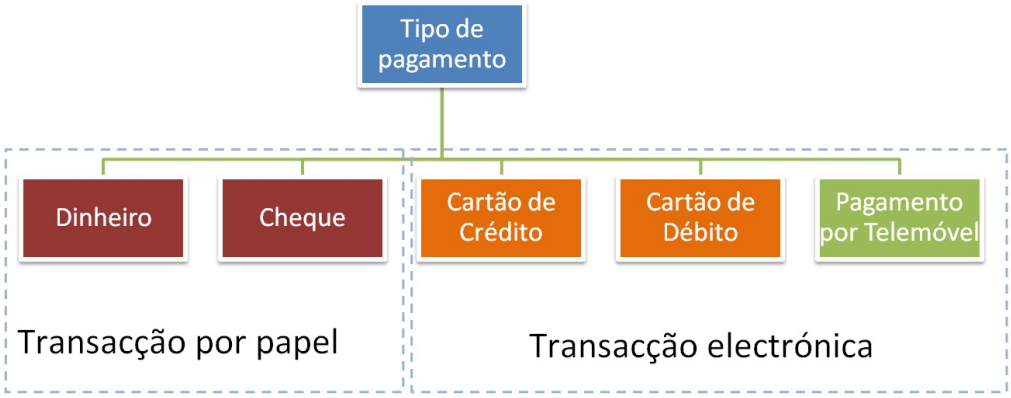

Figura 3.1: Sistema de pagamento - Genérico.

Contudo esta evolução tecnológica tem vindo a arrastar-se durante anos devido aos problemas de segurança inerentes à utilização do telemóvel como portador de bilhetes ou como elemento activo no sistema de pagamento. Mas o surgimento de novas tecnologias nesta área, como os *smart cards*, as *PKI* e o NFC antevêem novos desenvolvimentos no sistema de pagamentos num futuro próximo. Esta nova realidade possibilitará também às operadoras de redes móveis atingirem novos mercados, que até então eram dominados pelas instituições bancárias.

Figura 3.2: Novo sistema de pagamento.

3.2 Sistema de pagamentos

O sistema de pagamentos é constituído por diversos intervenientes, nomeadamente os bancos, os consumidores e o comerciante, sendo que o seu conjunto define uma cadeia, na qual fluem todas as informações sobre uma determinada compra ou venda de um determinado serviço. Seguidamente descrevem-se alguns sistemas relacionados que se enquadram neste sistema de pagamento convencional.

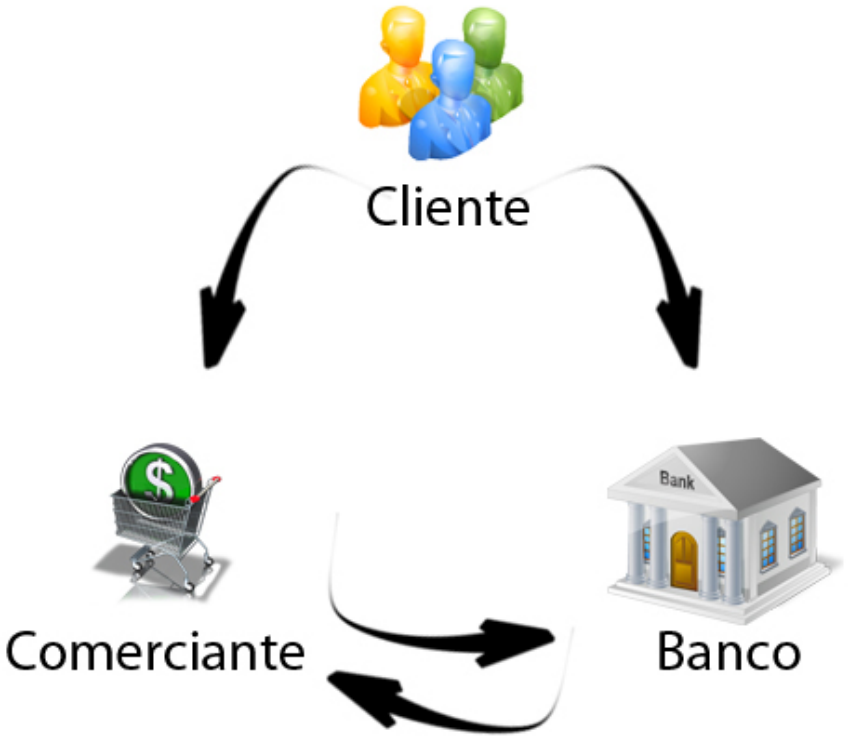

Figura 3.3: Ilustração do sistema de pagamentos.

3.2.1 Operadores de transportes

A larga maioria dos operadores de transportes, casos como a *OTLIS* (Operadores de transportes da área metropolitana de Lisboa - *http://www.otlis.com.pt/*) e a *Oyster* (Transportes de Londres - *https://oyster.tfl.gov.uk*) são casos de estudo interessantes dado que ambos os operadores utilizam algumas das tecnologias abordadas no capítulo anterior.

No caso da *OTLIS*, esta pela gestão dos transportes públicos de Lisboa. O método de pagamento utilizado pelos cidadãos para se poderem deslocar nos transportes consistem em adquirirem um cartão RFID pré-pago, este é o responsável por permitir o acesso aos terminais. O cartão normalmente pode ser adquirido nos balcões das companhias ou em quiosques, sendo que o método de pagamento pode ser dinheiro ou através de cartões multibanco e por isso o papel activo dos bancos.

Por sua vez, a *Oyster* utiliza a tecnologia dos *smart cards*, na variante de *Contactless Card*, com o mesmo método de funcionamento.
Nestes dois cenários, independentemente da tecnologia utilizada ser um factor vantajoso neste contexto devido à rapidez de processamento, ambos os casos se identificam no mesmo sistema de funcionamento e pagamento.

3.2.2 Bilhetes para espectáculos

A *TicketLine* é uma plataforma para a divulgação e comércio de bilhetes para eventos/espectáculos. Quando se pretende realizar uma compra de um bilhete para o evento, o utilizador acede ao sítio Internet (*www.ticketline.pt*) e depois deve seleccionar o espectáculo pretendido devendo realizar de imediato o seu pagamento. Este pagamento deve realizar-se através de cartão crédito, ou seja, neste caso as instituições financeiras têm de facultar a informação à *TicketLine* sobre a validade e a autenticidade do cartão. Uma vez confirmado, a *TicketLine* e as instituições financeiras notificam o utilizador que o pagamento foi realizado com sucesso. Deste modo facilmente se constata a relação indissociável entre todas as entidades que resulta no bom funcionamento do sistema.

3.2.3 A e-ID como parte do sistema de pagamentos

O caso do cartão *BankID* (*http://www.bankid.com*), implementado pela *Oberthur*, na Suécia, também é importante de analisar uma vez que permite constatar a relevância que os bancos dão a este tipo de sistemas. Neste caso, o cartão para além de representar o documento de entidade pessoal, este também é responsável por concluir a transacções.

Assim, o *BankID* na Suécia é o líder em identificação electrónica, tendo sido desenvolvido por um conjunto de grandes bancos com o intuito de serem utilizados por cidadãos, autoridades e empresas. Actualmente, é possível ser utilizado nos serviços governamentais, nos bancos e pelas empresas de um modo conveniente e seguro, graças à segurança oferecia pela PKI (Public Key Infrastructure) instalada no cartão.

O *BankID* é um sucesso na Suécia, sendo usado por mais de 2 milhões de pessoas tanto para a identificação, bem como para comércio electrónico, o que do ponto de vista da segurança relacionada com os sistema de pagamento esta é capaz de oferecer outro tipo de garantias. Por outro lado, em comparação com os casos de estudo referidos anteriormente e outros que fazem também parte deste sistema, esta solução dispensa a utilização de um outro cartão utilizado para a autenticação ou validação de um serviço.

3.3 Novo sistema de pagamentos

Após uma breve exposição sobre o sistema de pagamentos convencional e da apresentação de alguns casos de estudo, apresenta-se de seguida a evolução do mesmo. Assim, a evolução do sistema inclui uma nova entidade, as operadoras de redes móveis. Isto deve-se ao facto das potencialidades e da tecnologia em torno dos telemóveis possibilitar esta inclusão. Contudo existem inúmeras questões relacionadas com a privacidade e a segurança que devem ser tomadas em consideração.

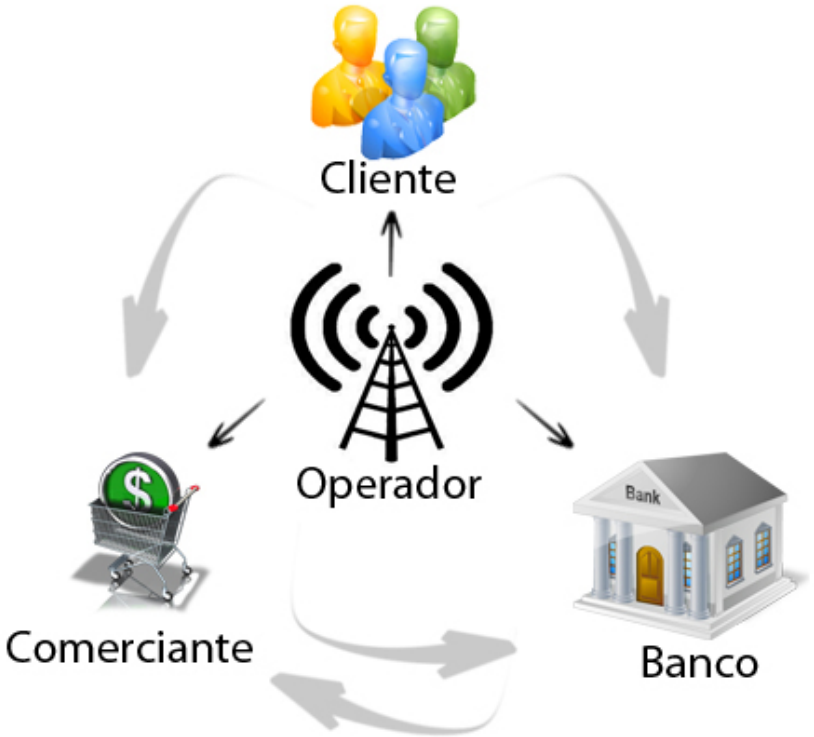

Figura 3.4: Ilustração do novo sistema de pagamentos.

Tal como se constata, um pouco por todo o lado existem várias entidades que tentam enquadrar o telemóvel como uma carteira digital que permita efectuar e realizar operações com dinheiro electrónico. Seguidamente apresentam-se alguns casos de como o telemóvel está a ser incluindo neste novo sistema de pagamentos.

3.3.1 Sistema - *M-Pesa*

Em Março de 2007, a maior companhia de telecomunicações do Quénia, a Safaricom (grupo Vodafone) lançou o *M-Pesa*.

O conceito do *M-Pesa* é bastante simples, consiste em que cada utilizador através do seu telemóvel possa movimentar pequenas quantias de dinheiro de forma segura. O desenvolvimento deste sistema deve-se à necessidade sentida pelos cidadãos, ou seja,

estes têm de se deslocar em grandes distâncias o que é dispendioso e leva bastante tempo. Deste modo, o *M-Pesa* não necessita que um cidadão possua uma conta num banco, mas sim uma conta *M-Pesa* e estar registado na Safaricom.

O método que utilizam para inserir dinheiro no telemóvel é realizado de forma semelhante aos agentes de pagamento em Portugal (*PayShop*), estes são os responsáveis por inserirem o dinheiro na conta *M-Pesa*, ficando estes com a total responsabilidade do dinheiro perante a operadora.
Por último, com o dinheiro no telemóvel é possível transferi-lo de uma conta para outra ou então pagas as compras num comerciante. O modo como se processa pagamento consiste numa simples transferência do saldo do telemóvel do cidadão para a conta do comerciante [33].

Figura 3.5: M-PESA [33]

3.3.2 *MB Phone*

O *MB Phone* é um serviço criado pela SIBS [67] que possibilita ao utilizador de um telemóvel realizar a maioria das transacções que estão disponíveis nas Caixas Automáticas, vulgo Multibanco. É possível realizar carregamentos de telemóveis (pré-pagos), pagamentos de serviços, consultas de saldos e movimentos bancários, consultas de NIB, pedidos de livros de cheques, transferência entre contas associadas e pagar compras realizadas na Internet.

Embora não se estabeleça uma ligação directa entre o consumidor e o comerciante, é possível através da Internet estabelecer-se esta ligação virtual a qual permite o pagamento de produtos e serviços através da rede multibanco, ficando esta com a missão de transferir os valores monetários para os comerciantes.

Figura 3.6: *MB Phone* [67]

3.3.3 Projectos - NFC

Os mais recentes desenvolvimentos da tecnologia possibilitaram o aparecimento da tecnologia NFC associada aos telemóveis. Desde então têm surgido inúmeros projectos-piloto na área da bilhética por parte de grandes empresas em diversas áreas, o que faz adivinhar uma nova era onde os telemóveis possuirão mais funcionalidades capaz de se assemelharem à carteira de um cidadão comum.

No que diz respeito, à sua inclusão no sistema de pagamentos sugerem algumas alterações portanto importa perceber o modo *operandis* deste tipo de tecnologia neste contexto.

A tecnologia baseia-se num *chip* NFC que comunica com os sistemas de pagamento por contactless (sem-fio) [20]. Assim, quando existe uma interacção com o telemóvel perto do leitor estabelece-se uma comunicação sem-fios onde os dados são trocados entre o leitor e o telemóvel, realizando-se desta forma os respectivos pagamentos de serviços através do telemóvel.

Figura 3.7: Visa NFC - Terminal Contactless.

Claramente que o acto de pagamento ao ser realizado por um telemóvel através da tecnologia NFC, terá que possuir mecanismos e elementos que tornem esta comunicação segura. Estes elementos são apresentados na imagem ilustrativa 3.8.

Figura 3.8: Elementos que compõem modelo NFC.

- *Universal Integrated Circuit Card*(UICC) - O elemento central dos telemóveis é o UICC, vulgo "cartão SIM"(*smart card*). É no cartão SIM que se entram as aplicações NFC que realizam as transacções electrónicas dos dados. A comunicação entre o cartão e as aplicações NFC é alcançado através da interface SWP (Single Wire Protocol), este protocolo baseia-se numa norma padrão para a comunicação entre o SIM e o *chip* NFC, suportado por mais de 52 operadoras móveis [35].

- *Secure Element* - Para habilitar este serviço, a aplicação de pagamento é inserida no SIM do cartão num ambiente seguro e controlado. Este factor é bastante importante na medida em que os dados transferidos via NFC do telemóvel para o terminal do comerciante são transmitidos às entidades financeiras que seguidamente processam as respectivas transacções monetárias.

- *Pay-Buy-Mobile* - Como resultado da utilização da tecnologia NFC nos telemóveis juntamente com o desenvolvimento de um cartão SIM capaz de comunicar com o *chip* NFC via o protocolo SWP, torna-se então possível de afirmar que é uma realidade realizarem-se pagamentos seguros através do telemóvel.

Ainda assim, após a fácil interpretação do funcionamento desta tecnologia, interessa observar as diferenças referidas anteriormente acerca do sistema de pagamentos.

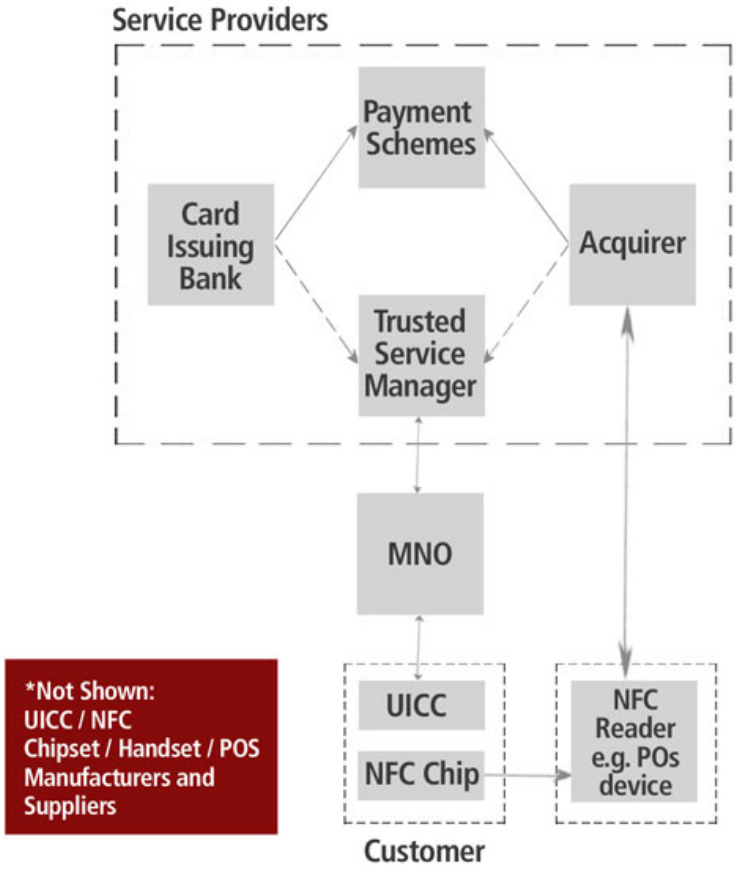

Figura 3.9: Ilustração sistema de pagamentos NFC [30].

Tal como mostra a figura 3.9, o sistema apresentado é bastante semelhante ao "novo sistema de pagamentos". Analisando mais cuidadosamente pode constatar-se que os bancos e as operadoras de redes móveis são os principais elementos que dominam o ambiente, mas a grande diferença que se pode visualizar é a inserção de um *Trusted Service Manager*, isto é, uma entidade que faz a gestão da comunicação entre os dados provenientes das operadoras, dos bancos e o próprio terminal NFC do comerciante.

3.3.4 Projectos - Códigos de Barras 2D

Como se apresentou no capítulo anterior, os códigos de barras 2D possuem diversas potencialidades que o tornam um elemento capaz de se integrar num sistema de pagamentos moderno. Dito isto, um dos projectos mais recentes nesta área surgiu numa parceria entre a Caixa Geral de Depósitos e a *Movensis* que apresentam uma solução que permite pagamentos através de dispositivos móveis e que recorre a duas tecnologias padrão: os SMS e os Códigos de Barras 2D.

Na prática, este sistema inicialmente vai estar restrito a máquinas de *vending* (chocolates, cafés) que tenham aderido ao sistema, sendo que as mesmas devem possuir um modem GSM acoplado para receber os créditos do cliente. Dito isto, para se realizar uma compra é necessário o cliente introduzir um PIN para aceder à aplicação no telemóvel e de seguida enviar uma SMS para o sistema com os dados relativos ao número de série da máquina, que por sua vez se encontra registada no ecossistema.

A empresa pretende ainda incluir a compra de bilhetes para eventos através do telemóvel, os quais são recebidos no formato de código de barras 2D que podem ser lidos através dos terminais de leitura dos comerciantes. Mais detalhes sobre este projecto podem ser consultados em [34].

Importa ainda referir que este sistema é semelhante em alguns aspectos ao sistema *Ticket-ID*, contudo este projecto em particular será analisado e comparado com o sistema *Ticket-ID* no capítulo 8.

3.3.5 Futuro do sistema de pagamentos

Analisados alguns sistemas similares importa perceber como responder a questões de segurança existentes e a novas que se possam colocar dada a crescente inovação nestas áreas.

Neste momento, como se descreveu os sistemas de pagamento incluem uma nova entidade, as operadoras de redes móveis, e como tal este facto não deve ser ignorado

pois o futuro passará por centralizar o máximo de operações no telemóvel. Como tal, elas são um elemento fundamental para a construção do futuro das transacções electrónicas, o que mudará definitivamente o quotidiano das pessoas.

Porém a centralização de todos os serviços na nova carteira digital (telemóvel) levanta grandes preocupações em termos de segurança, privacidade e de tecnologia, uma vez que, a maioria dos utilizadores utilizam o telemóvel para realizarem pequenas transacções o que do ponto de vista da operadora móvel significa grandes volumes de comunicações de dados que envolvem pequenos valores monetários associados. Contudo para se inverter esta situação é necessário perceber como garantir, por exemplo, que o simples roubo do telemóvel não afectará todo o sistema.

3.3.6 Características e Desafios

Importa perceber quais as características e os desafios que se colocam à implementação do novo sistema de pagamentos, tendo em conta a sua centralização no telemóvel [32].

- Rapidez de processamento - velocidade com que se realizam as operações de forma a evitar fila no processo de validação.
- Inovação - as entidades envolvidas devem desenvolver serviços inovadores para atrair a atenção das pessoas.
- Custos de manutenção - como qualquer outro sistema existem custos de manutenção, no entanto, este deverá ser auto-suficiente.
- Investimento em infra-estruturas - entidades bancárias não terão problemas em instalar novas infra-estruturas tecnológicas, mas no caso dos pequenos e médios comerciantes os custos são mais sentidos o que poderá provocar desigualdades competitivas no mercado.
- Investimento nas tecnologias (NFC) - o acesso a novos serviços está dependente da tecnologia usada. Assim, para um investimento equilibrado os custos devem ser repartidos por todas as entidades, nomeadamente pelas operadoras e pelos bancos.

- Universalidade do sistema - o sistema deve ser implementado segundo as mesmas normas/*standards* , resultando numa interoperabilidade global de modo a facilitar a integração da tecnologia junto da sociedade (ex: NFC).

- Facilidade de utilização - o sistema deverá ser capaz de ser facilmente compreendido, sobretudo a interface do sistema no telemóvel.

- Segurança - em termos de segurança devem salvaguardar-se os dados e a privacidade do utilizador, pois sem a sua confiança todo o sistema poderá ser ameaçado.

- Resiliente a ataques - deve ser sólido aos mais diversificados ataques, tanto a nível de tecnológico como de engenharia social.

- Cooperação entre entidades - o sistema ao ser composto por diferentes entidades, estas devem mostrar um bom relacionamento e uma boa cooperação pois é essencial para o sucesso do sistema.

- Certificação das entidades - tal como acontece actualmente todas as entidades devem ser certificadas de acordo com todos os requisitos e parâmetros de segurança, de forma a existir uma cadeia de confiança entre todos os intervenientes.

3.4 Segurança e Privacidade

Após uma análise genérica sobre as tecnologias envolvidas, o futuro do sistema de pagamentos e os desafios colocados, é necessário tecer algumas considerações em torno da segurança. Deste modo, em termos de privacidade, as informações pessoais armazenadas nos telemóveis ou em base de dados devem ser protegidas, nomeadamente o nome, data de nascimento, incluindo os identificadores biométricos (por exemplo, impressões faciais, impressões digitais), bem como as credenciais (passwords) pessoais e informações sobre as suas deslocações/movimentações.

Em termos de segurança informática, os telemóveis estão sujeitos ao mesmo tipo de ataques(*vírus*, *trojans*) que os computadores, devido a serem uma unidade de computação móvel e como tal também estão sujeitos ao mesmo tipo de vulnerabilidades, por exemplo ataques de *Phising* também são possíveis de suceder neste contexto e

como tal importa encontrar as respostas certas [17].

Existem ainda outras questões de segurança relacionadas com os múltiplos canais de autenticação utilizados para realizar autenticações ou pagamentos através do telemóvel, ou seja, actualmente existem diferentes métodos de pagamento que resultam das diferentes tecnologias utilizadas (NFC, Internet, Bluetooth, entre outros) e obviamente cada uma tem seus próprios mecanismos de segurança associados (PIN, Password, OTP, Certificados, *SIM-PKI*, Hardware token, entre outros [45], e como tal importa perceber as vantagens e as limitações destes mecanismos de segurança no sistema de pagamentos.

3.5 Resultados e Conclusões

Seguidamente apresenta-se uma tabela que foi construída para sintetizar e comparar os mecanismos de segurança mais usados actualmente, esta torna assim possível retirar algumas conclusões(genéricas) que serão úteis para o desenvolvimento do sistema *Ticket-ID*.

Tal como se pode observar da tabela 3.1, a melhor tecnologia em termos de segurança são os cartões SIM com Estruturas de Chaves Pública (PKI) capazes de usufruírem das vantagens da criptografia assimétrica. Contudo, esta solução também apresenta algumas preocupações, nomeadamente em relação à necessidade de memorizar um PIN sempre que for utilizada. Por outro lado, do ponto de vista do mercado, ainda não estão disponíveis actualmente estes cartões no mercado, ficando a dúvida sobre seus custos e sobre a facilidade de utilização por parte da sociedade.

Tabela 3.1: Comparação dos métodos de segurança mais utilizados

	 OTP via SMS	 SIM-PKI	 Token OTP	 Cartão PIN
Dispositivos utilizados	Telemóvel	Telemóvel + *SIM-PKI*	Telemóvel + token	Telemóvel + PINs
Múltiplas Aplicações	Sim, mas difícil	Sim	Não	Não
Facilidade de utilização	Novos códigos em cada utilização	PIN sempre que se utiliza	Novos códigos em cada utilização	Novos códigos em cada utilização
Custos do equipamento	Baixos, suportado pela operadora	Baixos, suportado pela operadora	Médios, responsabilidade do banco	Médios, responsabilidade do banco
Limites da tecnologia	Operadora para receber OTP	Possuir o *SIM-PKI* e Internet	Funciona a bateria	Os PINs devem ser renovados
Custos de implementação	Não apresenta	O preço do SIM e da logística	O valor do dispositivo	Gastos de envio no correio
Níveis de segurança	Médio/Alto implica ter um gerador de códigos num ambiente seguro	Alto devido à estrutura PKI	Médio/Baixo implica sincronização, facilmente roubado	Baixo, facilmente roubado ou copiado
Resistência a ataques	Sujeito a ataques de Eng.Social (Médio)	Resistente	Sujeito a ataques de Eng.Social (Médio)	Sujeito a ataques de Eng.Social (Fácil)

Embora a *Gemalto* esteja a desenvolver estes cartões capazes de suportarem a tecnologia NFC e simultaneamente os mecanismos mais avançados em termos de segurança através duma plataforma designada *DESFire* que possui os algoritmos criptográficos(*3DES, AES*) [24], surgem novos desenvolvimentos em termos de segurança bastante interessantes. Nomeadamente, as potencialidades associadas aos cartões de identidade electrónicos (*e-ID*) com os telemóveis, surgindo assim o mais recente elo de ligação entre estas duas tecnologias. Esta ligação possibilitará inserir no contexto dos sistemas de pagamento os melhores mecanismos de segurança associados aos *e-ID* (PKI, assinaturas, certificados, etc).

Dito isto, importa referir que esta ligação deve-se ao facto de actualmente os telemóveis serem vistos como a identidade em movimento, devido às inúmeras funcionalidades que requerem a autenticação pessoal. Tendo isto em conta então pode afirmar-se que a identidade pessoal é o coração das transacções seguras e de confiança.

	 e-ID + PKI e Assinatura
Dispositivos utilizados	Telemóvel + *e-ID*
Múltiplas Aplicações	Sim
Facilidade de utilização	Inserir o PIN quando necessário
Custos do equipamento	Baixos
Limites da tecnologia	Renovar *e-ID*
Custos de implementação	Novos terminais de leitura nos comerciantes
Níveis de segurança	Alto devido à estrutura PKI associada ao *e-ID*
Resistência a ataques	Resistente

Tabela 3.2: Método de segurança baseado na identificação electrónica

Claramente que as capacidades de segurança dos *smart cards* (*e-ID*), mais concretamente a infra-estrutura PKI, os certificados armazenados e as capacidades de assinatura digital associadas ao cartão, permitem que os pagamentos e autenticações a partir dos telemóveis usufruam destas características de segurança.

Como resultado desta associação de tecnologias apresentam-se dois casos de sucesso, o *FINEID* da Finlândia e o *Mobiil-ID* da Estónia.

3.5.1 Caso de estudo - *FINEID*

Apresenta-se em primeiro lugar o novo documento de identificação electrónica desenvolvido pelo governo Finlandês intitulado de *FINEID*.

Figura 3.10: Cartão de cidadão Finlandês [4].

O cartão *FINEID* consiste num *smart card* com *chip* com todos os aspectos físicos constituintes de um documento de identificação pessoal (nome, fotografia, data nascimento, assinatura, etc). No *chip* estão armazenados dois certificados, um para autenticação e outro para a assinatura digital.

A implementação do *FINEID* suporta ainda a funcionalidade de *SIM-PKI*, desenvolvida pela *SmartTrust* - *http://www.smarttrust.com*. A sua adesão por parte da população finlandesa está dependente de uma subscrição junto de uma operadora de rede móvel que suporta o serviço e fornece os cartões *SIM-PKI*. Os cartões contêm um par de chaves para autenticação e assinatura, sendo que os respectivos certificados são gerados e registados oficialmente (pelo centro de registo da população-finlandês) após o registo do cartão SIM numa esquadra policial [56].

Na prática, o cartão *SIM-PKI* pode ser utilizado para determinados fins, apresenta-se um exemplo de autenticação de um cliente num *web service* via telemóvel [4].

1. O utilizador através da Internet no seu telemóvel tenta aceder a um serviço (*service provider*) que requisita informações sobre o telemóvel (número) que esta a tentar aceder ao respectivo serviço.

2. O *webservice* após receber os dados envia um pedido de assinatura, que contem o número do telemóvel para a operadora.

3. A operadora envia o pedido de assinatura para o telemóvel do utilizador (*SIM-PKI*), no qual é gerada uma assinatura *PKCS♯1* através da respectiva chave privada do cartão (o utilizador insere o Código PIN para aceder à chave privada).

4. A assinatura e a *hash* da chave pública é enviada para a operadora, sendo ainda a assinatura embutida no pacote *PKCS♯7* que contem o certificado do utilizador.

5. A validação consiste com que a operadora verifique a respectiva assinatura, caso se verifique correctamente esta informa o *service provider* do sucesso da operação.

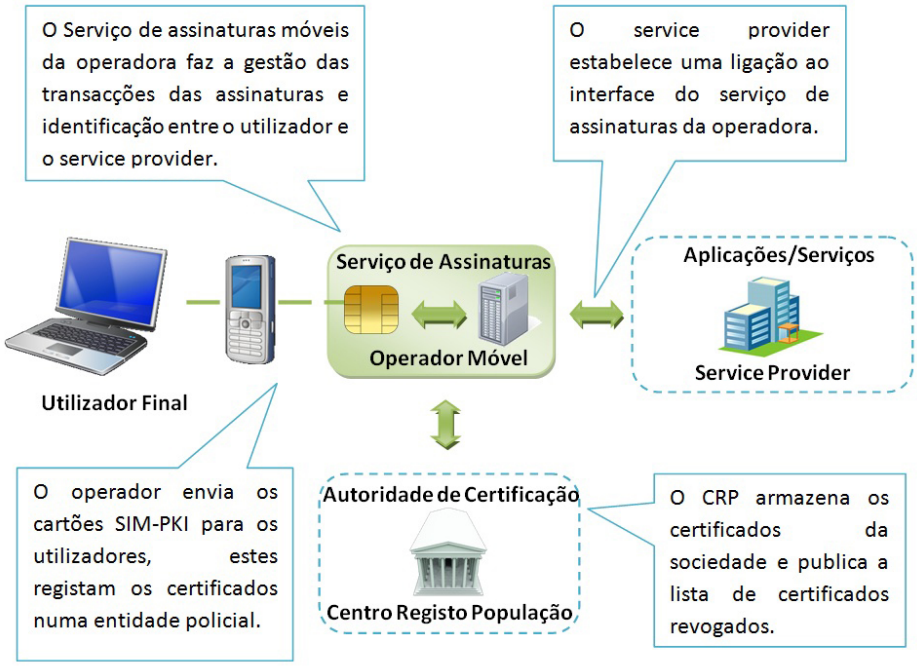

Figura 3.11: Plataforma PKI implementada na Finlândia.

O sucesso da interligação do telemóvel à identidade pessoal, permitiu ainda ao governo finlandês desenvolver uma plataforma aberta de pagamentos baseada no cartão *FINEID*. Esta plataforma possibilita a compra de bilhetes para os transportes públicos, utilizando no telemóvel os cartões *SIM-PKI*. Assim, a relação directa que existe entre o *FINEID* e o cartão SIM é simplesmente a estrutura PKI na qual assenta toda a plataforma de segurança.

3.5.2 Caso de estudo - Estónia *e-ID*

Em relação à Estónia, importa desde já destacar a simplicidade e a confiança que os cidadãos daquele país depositam no sistema de identidade nacional, isto porque muitos serviços como os transportes públicos são possíveis de utilizar recorrendo simplesmente à identificação pessoal.

Figura 3.12: Cartão de cidadão da Estonia [28] .

O sistema implementado que associa a identidade electrónica (*e-ID*) aos telemóveis designa-se de *Mobiil-ID*. Um cidadão daquele país que pretenda utilizar as novas funcionalidades deste novo sistema tem de subscrever um contrato do serviço *Mobiil-ID* junto de uma operadora de rede móvel. Após a subscrição desse serviço a operadora fornece um novo cartão SIM para o telemóvel do cidadão que deve ser activado em, *www.id.ee*, usando o seu cartão de identificação electrónico.

A activação do mesmo é necessária para garantir a segurança máxima do serviço, uma vez que este tem associadas as mesmas credenciais que o cartão de identificação, o que concede ao cidadão o acesso às suas contas bancárias e a capacidade de assinar

documentos judicialmente vinculativos. Este novo cartão SIM tem mais funcionalidades, como por exemplo, os códigos necessário para a identificação através da Internet e possibilita ainda assinar documentos digitalmente [43].

Apresenta-se na figura 3.13 o sistema de bilhética da Estónia, podem ainda ser vistas as potencialidades do *Mobiil-ID* em [27] .

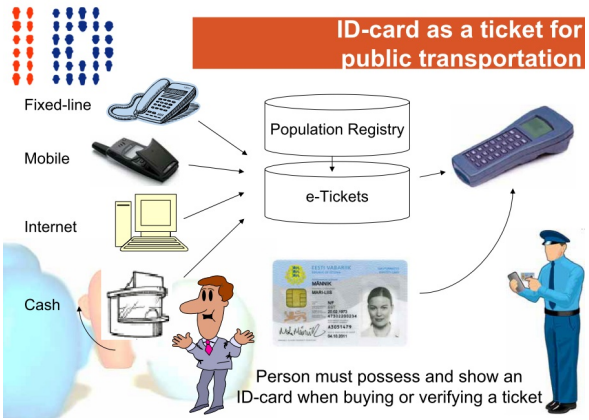

Figura 3.13: Ecosistema de bilhética na Estónia [43] .

Actualmente na Estónia é possível votar através de um computador com Internet, contudo a utilização do telemóvel será vista como uma alternativa capaz de simplificar a autenticação do acto eleitoral, dado que as politicas internas de determinados locais não permitem a utilização de leitores de cartões ou até mesmo a leitura de cartões de identificação [59]. Num futuro próximo a plataforma *Mobiil-ID* vai possibilitar a utilização do telemóvel em actos eleitorais, ainda assim esta nova meta revela-se um grande desafio.

Em termos de segurança o *Mobiil-ID* já foi alvo de uma análise formal por *Laud* e *Roos* [41]. No que diz respeito em concreto ao acto eleitoral, a Estónia não vai permitir para já o uso do telemóvel para todos os processos eleitorais devido a preocupações com a segurança do processo.

Capítulo 4

Ticket-ID projecção e idealização do sistema

Neste capítulo, apresentam-se as características idealizadas para o sistema *Ticket-ID* tendo em conta o estado da arte e a análise realizada sobre os sistema relacionados. No entanto, antes de se descreverem as mesmas é essencial fazer-se um ponto de situação para que se tenha uma ideia mais clara e consistente das informações apreendidas até aqui.

4.1 Considerações importantes

Actualmente os telemóveis são dispositivos com uma enorme mobilidade e encontram-se em constante conectividade, onde o acesso a novos serviços está dependente das credenciais de autenticação e identificação do utilizador.

Como se apresentou, existem importantes questões de segurança associadas a estas novas potencialidades, contudo alguns projectos-piloto, como o caso da Finlândia ou da Estónia, demonstram como é possível **associar as credenciais da identidade pessoal ao telemóvel**.

Tendo em conta que milhões de pessoas fazem diariamente inúmeras autenticações e muitas delas através do documento de identificação pessoal, sem dúvida que a credibilidade associada a este documento e a sua associação a outras tecnologias (telemóveis)

torna possível o desenvolvimento de novos produtos inovadores e de confiança para a sociedade. Por outro lado, esta associação (telemóvel/identificação) apenas é possível devido a projectos tais como o *STORK*, que permitem a existência de uma plataforma de interoperabilidade entre *e-ID* de diferentes países.

Em relação às tecnologias mais utilizadas juntamente com o telemóvel, a análise dos sistemas similares, permitiu destacar o NFC e o *QR-Code*. Ambas apresentam uma utilização bastante simples e computacionalmente de rápida execução. No caso do NFC, este tende a basear-se numa estrutura *SIM-PKI* ao longo do processo de pagamento. Em relação ao *QR-Code*, a quantidade de informação possível de armazenar e a diversidade da sua possível utilização são factores muito importantes.

Dito isto, qualquer sistema inovador que se projecte não deve ficar refém apenas de uma única tecnologia por diversas questões, mas principalmente pelo facto que a dependência excessiva de uma tecnologia poderá limitar o sistema em termos de utilização.

Na vertente do sistema de pagamentos, este deve estar bem definido pois actualmente decorrem modificações nas tendências do mercado e deste modo as vantagens associadas a cada entidade devem ser tidas em consideração.

Nestes termos definiu-se que o sistema idealizado deve integrar o cartão de cidadão português como tecnologia fundamental do sistema. Por outro lado a interligação do mesmo com outras tecnologias, nomeadamente o NFC, *QR-Code* e os telemóveis sugerem um sistema inovador, simples, seguro e sustentável.
Apresenta-se de seguida a estrutura idealizada, mais precisamente o ciclo de vida de um bilhete.

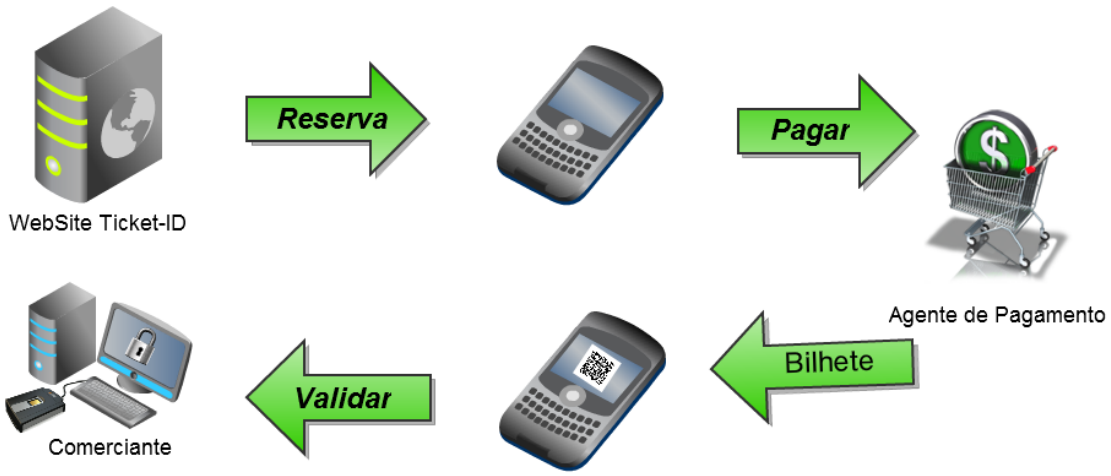

Figura 4.1: Arquitectura da plataforma *Ticket-ID*.

4.2 Idealização do sistema a nível tecnológico

No que diz respeito às tecnologias a utilizar, apresentam-se as características:

- NFC:
  - Interacção com os terminais dos agentes de pagamento e do comerciante por telemóvel ou por cartão contactless.
  - Na utilização por cartão contactless, este deve ser capaz de armazenar o bilhete (assinatura digital).
  - No telemóvel (NFC) o software deve ser simples e intuitivo.
- **QR-Code:**
  - Representação do bilhete (assinatura digital).
  - Armazenar um URL para aceder a uma representação digital do bilhete através da Internet.
  - Interacção com os terminais do comerciante através de telemóvel, por impressão em papel e por *WebCam*.

- ***Smart Card - Cartão de Cidadão:***
  - Armazenar parte do bilhete (*Hash*).
  - Interacção com os terminais dos agentes de pagamento e do comerciante através de um leitor de cartões e impressão digital.
  - Gestão da área pública do cartão de cidadão, salvaguardando os dados pessoais e a confidencialidade dos mesmos.

4.3 Idealização do sistema de pagamentos

No que diz respeito ao sistema de pagamentos, tal como foi referido anteriormente o sistema foi idealizado de acordo com o "novo sistema de pagamentos", apresentam-se as seguintes características correspondentes a cada elemento:

- **Operadora de rede móvel:**
  - Responsável por gerir o envio das SMS com as referências de pagamento.
  - Responsável por gerir o envio das MMS com os bilhetes no formato *QR-Code*.
- **Agente de Pagamentos:**
  - Valida as referências do cliente, por observação visual da SMS ou electronicamente por NFC.
  - Realiza as operações criptográficas de construção do bilhete através das credenciais do cartão de cidadão.
  - Realiza a codificação do bilhete no formato de código de barras 2D - *QR-Code*.
  - Possibilita a gestão da área pública do cartão de cidadão.
- **Comerciante:**
  - Realiza a validação dos bilhetes recebidos de três formas possíveis: via NFC, leitura código barras e *WebCam*.

  - Faz a devida gestão do sistema consoante o tipo de validação do bilhete, simples ou forte.

- **Cliente:**

  - Efectua uma reserva ou uma compra directa usando os meios de pagamentos habituais.
  - Recebe o bilhete no telemóvel utilizando a tecnologia seleccionada.
  - Realiza a validação do bilhete no comerciante.

4.4 Idealização do sistema de informação

No que diz respeito, ao sistema de informação este representa a base de todo o sistema. De seguida descrevem-se as suas respectivas características:

- Gestão automática diária de eventos(espectáculos).
- Alerta e gestão de eventos.
- Interface agradável ao utilizador.
- Gestão da área pública do cartão de cidadão.
- Serviço de reserva de bilhetes.
- Gestão de reservas.
- Autenticação dos utilizadores.
- Interfaces dinâmicas consoante os utilizadores.
- Inclusão de elementos multimédia sobre os eventos.

4.5 Avaliação do sistema idealizado

Após a idealização do sistema torna-se necessário avaliar os parâmetros definidos. Esta fase contou com a participação da empresa *Multicert*, especialistas em segurança e/ou certificação digital para todo o tipo de transacções electrónicas. Deste modo

apresenta-se uma listagem que demonstra a avaliação realizada ao sistema idealizado. Importa referir que a avaliação foi realizada de acordo com as características e os desafios referidos na secção 3.3.6.

Assim, apresentam-se aqui as respostas que o sistema *Ticket-ID* terá que ser capaz de dar aos respectivos desafios:

- Rapidez de processamento: A tecnologia NFC e código de barras apresentam tempos de processamento/comunicação bastante rápidos para as várias operações.
- Inovação: a inovação proporcionada pela introdução do cartão de cidadão e das novas tecnologias associadas ao telemóvel, torna o sistema bastante inovador.
- Custos de manutenção: o ciclo de vida do sistema é auto-suficiente pois toda a plataforma é suportada por um simples sistema de informação e por dispositivos electrónicos de custo reduzido.
- Investimento em infra-estruturas: no que diz respeito ao agente de pagamento os custos são reduzidos pois terá que possuir apenas um leitor de cartões com suporte da tecnologia NFC. Em relação ao comerciante este terá que possuir também um leitor de cartões e um leitor de códigos de barra 2D ou uma *WebCam*, ainda assim são os valores são reduzidos.
- Investimento nas tecnologias: em relação ao cartão de cidadão a sociedade na sua grande maioria já adquiriu o mesmo para outros fins e como tal não representa um custo adicional. Por sua vez o telemóvel terá de possuir a tecnologia NFC, mas este facto não implica a necessidade obrigatória de aquisição de um novo equipamento por dois factores: em primeiro lugar existem cartões SD que suportam o *chip* NFC, o qual pode ser acoplado ao telemóvel; outro factor é que pode ser sempre utilizada a tecnologia do código de barras que não apresenta nenhum custo.
- Universalidade do sistema: esta pode ser garantida graças a projectos como por exemplo o STORK [77], e suas plataformas de interoperabilidade.
- Facilidade de utilização: grande simplicidade graças à tecnologia sem-fios, por outro lado a tecnologia de código de barras é bastante simples e intuitiva. Em

relação às aplicações usadas no telemóvel, estas devem ser projectadas de acordo com todos os parâmetros de simplicidade.

- Segurança: este sistema baseia-se nas credenciais do cartão de cidadão, mais precisamente na sua estrutura PKI, a qual será abordada tecnicamente mais adiante.
- Cooperação entre entidades: a cooperação entre as entidades envolvidas no sistema é bastante linear, uma vez que o fluxo de informação entre todas assenta no sistema de informação (base de dados) e como tal está sempre actualizada e disponível em tempo real a todos os intervenientes.
- Certificação das entidades: a implementação do sistema deve contemplar a certificação dos intervenientes de forma a ser garantida a confidencialidade dos dados e a privacidade do utilizador ao longo de todo o sistema. Tornando assim possível salvaguardar o bom funcionamento do sistema num ambiente seguro e controlado.
- Resiliente a ataques: as respostas que o sistema dará aos possíveis ataques de que será alvo serão capazes de determinar a solidez da camada de segurança do sistema.

4.6 Objectivos definidos

Apresentam-se os objectivos definidos para a elaboração do sistema *Ticket-ID*.

Assim, em relação aos objectivos definidos o sistema deve possuir uma base de informação centralizada capaz de gerir todas as informações sobre eventos/espectáculos e os respectivos bilhetes. O uso da tecnologia NFC e *QR-Code* são essenciais para que o fluxo de informação entre todas as entidades seja processado rapidamente. Por outro lado, os telemóveis são importantes uma vez que são estes os responsáveis por transportar os bilhetes entre todas as entidades.

Em relação à camada de segurança do sistema, esta deve basear-se na utilização do cartão de cidadão, nomeadamente nas capacidades criptográficas de autenticação e assinatura do mesmo, de modo a desenvolver-se um sistema fortemente seguro, tornando

assim possível **a associação da identidade pessoal ao bilhete electrónico**.

Por último, pretende-se que a camada de segurança seja flexível ao ponto de ser possível suportar diferentes ambientes de validação. Neste caso, deve suportar as validações:

- **Simples** - casos onde é necessária uma autenticação rápida e segura do bilhete (ex: transportes públicos).
- **Forte** - situações onde é necessário garantir a segurança máxima em relação à autenticidade do bilhete, para isso é necessária a utilização do cartão de cidadão como elemento de prova (ex: Jogo de futebol - campeonato do mundo).
- **Extra Forte** - casos específicos onde é necessário garantir para além da autenticidade do bilhete a identidade do portador do cartão de cidadão (ex: bilhete de avião).

4.7 Conclusão

Em suma, este capítulo define um esboço bastante avançado do sistema a desenvolver e dos objectivos a alcançar. Ainda assim importa referir que a principal inovação do projecto não se baseia na produção de um novo sistema de bilhética, mas sim na originalidade da utilização do cartão de cidadão na camada de segurança do sistema.

Pode-se ainda concluir que a utilização do cartão vem solucionar alguns problemas constatados nos sistemas similares. Veja-se por exemplo o caso dos transportes públicos onde o telemóvel é utilizado juntamente com a tecnologia NFC para validar o acesso aos mesmos. Neste ambiente são possíveis de existirem ataques de *Phishing* ao telemóvel ou até mesmo o furto do telemóvel é apetecível, uma vez que as pessoas e os sistemas de informação armazenam informações sensíveis sobre os serviços utilizados bem como as respectivas credenciais.

Neste contexto, a capacidade de associar o cartão de cidadão ao sistema permite responder de forma eficaz ao problema dos furtos, dado que o bilhete que se encontra no telemóvel e no *QR-Code* é simplesmente uma *assinatura digital*. Deste modo,

o atacante não consegue identificar a origem ou o serviço onde utilizar de forma proveitosa e indevida o telemóvel(bilhetes).

Finalmente, importa ainda referir que em termos de segurança outras questões podem ser levantadas, mas nesse caso são muito provavelmente aspectos relacionados com o cartão de cidadão. O que na realidade as torna questões sobre a tecnologia dos *smart cards* e como tal existe uma preocupação mundial devido às entidade envolvidas, o que permite que possam ser encontradas mais rapidamente as melhores respostas.

No próximo capítulo, descreve-se a arquitectura da plataforma *Ticket-ID*, o que vai permitir perceber como se atingiram os objectivos definidos neste capítulo e a sua real importância.

Capítulo 5

Arquitectura do sistema *Ticket-ID*

O presente capítulo descreve a arquitectura do sistema tendo em conta a solução proposta e os objectivos definidos no capítulo anterior. Deste modo a abordagem seguida ao longo do processo de desenvolvimento da arquitectura, consistiu fundamentalmente numa investigação e na análise funcional do sistema idealizado. Desta análise resultaram diferentes cenários de utilização consoante os intervenientes em causa.

Como resultado, foi possível dividir a arquitectura em pequenos módulos, possibilitando a implementação do sistema de acordo com as necessidades e os objectivos definidos. No entanto, esta abordagem provou-se bastante útil, na medida em que é possível o desenvolvimento independente de cada um dos módulos, o que na prática permite uma manutenção muito mais simples.

Seguidamente apresenta-se um diagrama que ilustra a arquitectura do sistema desenvolvido de forma a simplificar a percepção e entendimento do sistema, o qual será descrito detalhadamente.

5.1 Descrição do sistema

Tal como mostra o diagrama da figura 5.1, este apresenta a arquitectura do sistema na qual estão descritos todos os passos ao longo do ciclo de vida de um bilhete. No entanto, importa referir que também é possível realizar a compra de bilhetes directamente no agente de pagamento, tal facto não altera em nada o ciclo de vida do bilhete.

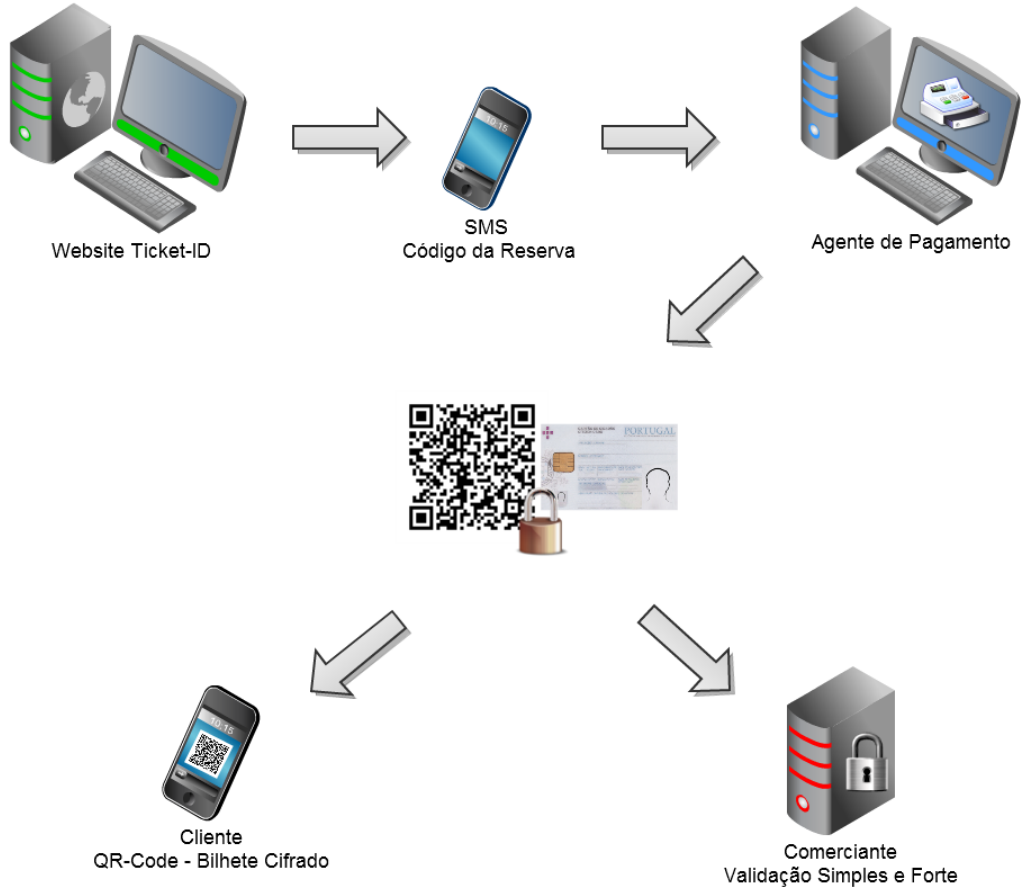

Figura 5.1: Arquitectura do sistema *Ticket-ID*.

Considerando o ciclo de vida completo do bilhete, em primeiro lugar o cliente efectua uma reserva para um determinado evento através do website *Ticket-ID* e recebe no seu telemóvel uma SMS com a referência de pagamento do bilhete reservado(opcional) e um email do sistema com os respectivos dados.
Seguidamente o cliente terá que se dirigir a um agente de pagamento (ex:*Payshop*) à qual faculta a respectiva referência via NFC ou por observação visual da SMS.

O agente de pagamento é a entidade responsável por "construir o bilhete". O processo de construção pode variar consoante o tipo de validação (simples/forte) definido pelo comerciante para o evento em causa. No entanto, independentemente do tipo de validação, o agente de pagamento necessita que o cliente lhe faculte o seu cartão de cidadão para poder associar a sua identificação pessoal ao bilhete.

Após a construção do bilhete o agente de pagamento envia ao comerciante e ao cliente os dados relativos à venda do respectivo bilhete(comprovativo). Estes podem ser enviados de duas formas para o cliente, via MMS com um *QR-Code* que representa o bilhete ou via NFC directamente para o telemóvel do cliente.

Finalmente, a validação do bilhete também se pode realizar de duas formas: do tipo forte, onde são requeridas mais credenciais pessoais ao portador do bilhete; do tipo simples, neste caso apenas são validados os bilhetes independentemente do portador dos mesmos. Contudo, isto implica que consoante o tipo de validação definida para o evento, o consumidor tenha que possuir o bilhete recebido e o seu cartão de cidadão.

Tal como se referiu no início deste capítulo, esta arquitectura dividiu-se em pequenos módulos. Cada um dos módulos diz respeito a cada uma das fases ao longo do ciclo do bilhete, isto é: a fase de reserva de bilhetes - Módulo página Web; o processo de pagamento - Módulo do agente de pagamento; fase de validação do bilhete - Módulo do comerciante.

A implementação do sistema em módulos, permite encontrar as melhores soluções para os objectivos definidos. Deste modo a manutenção e a actualização do sistema é mais eficiente graças à flexibilidade que cada um dos módulos permite, ou seja, na prática qualquer tarefa de manutenção ou alteração do sistema num dos módulos não implica obrigatoriamente modificar e alterar todos os outros.

Seguidamente descreve-se cada um destes módulos e os respectivos aspectos técnicos, no final apresenta-se a camada de segurança associada a cada um deles.

5.1.1 Módulo da plataforma de venda - *Website*

O primeiro módulo desenvolvido do sistema foi uma plataforma *Online* de reserva de bilhetes para diversos eventos à semelhança dos serviços, *TicketLine* e *Ticketmaster*. Embora seja possível que um comerciante possa integrar a plataforma *Ticket-ID* no seu próprio website recorrendo à tecnologia de serviços web.

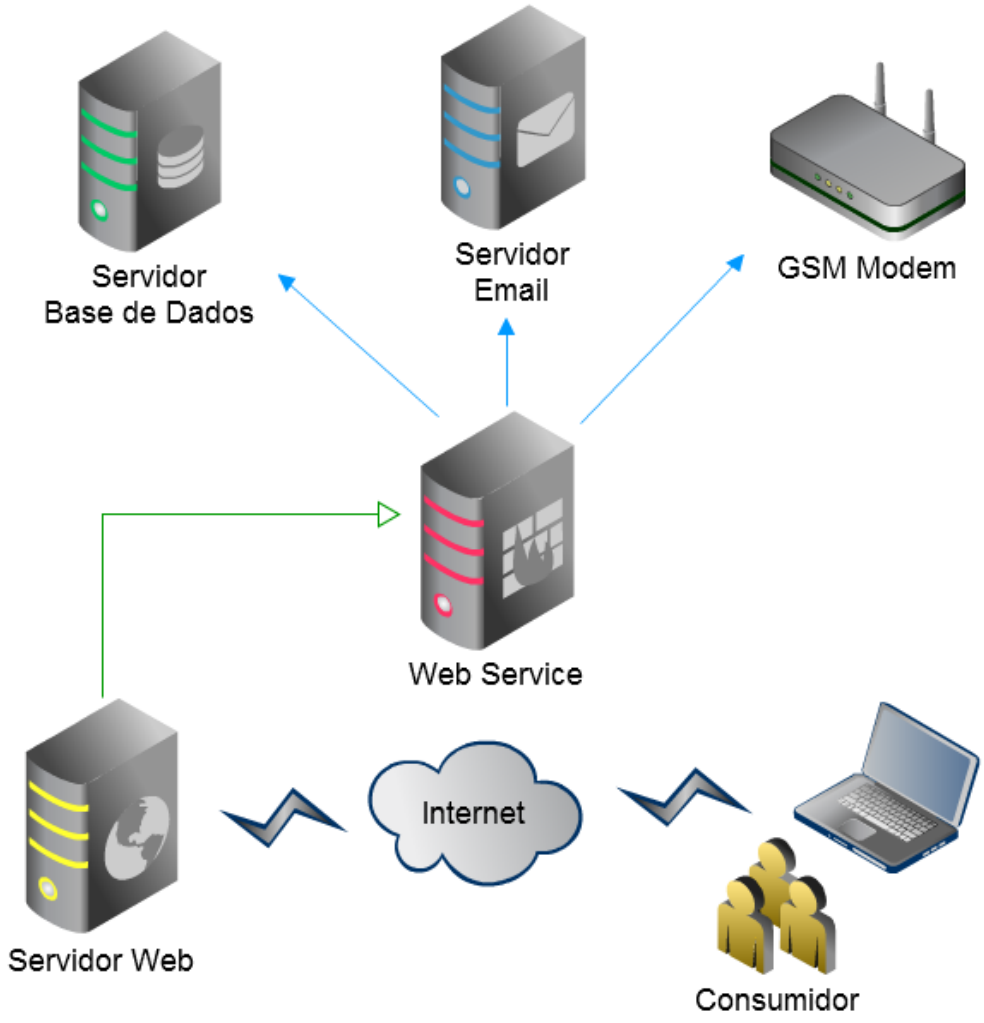

Figura 5.2: Diagrama com a arquitectura do sistema de vendas/reservas.

Tendo em conta que a plataforma *Online* desenvolvida contempla diversos elementos de computação torna-se importante descrever a abordagem seguida no desenvolvimento de cada um deles.

- ***WebService:*** o seu desenvolvimento permite que o sistema seja independente da tecnologia utilizada, isto é, através dele é possível aceder às funções pré-definidas do sistema sem que para isso seja necessário reprogramar as mesmas (ex: realizar login). Este comunica também com os outros servidores, nomeadamente, o de base de dados, email e o com o modem GSM de forma transparente. Em suma, o *WebService* permite centralizar todo o sistema, dado que este é o principal responsável por estabelecer a comunicação entre todos os elementos.

- ***Servidor de Base de Dados:*** o servidor de base de dados é onde se encontra armazenada a informação sobre os clientes, comerciantes e respectivos eventos. Este servidor na prática armazena toda a informação do sistema, motivo pelo qual a sua implementação, manutenção e segurança seja muito importante.

- ***Servidor de Email:*** a implementação do servidor de email consiste no simples facto de ser importante enviar novos alertas para o cliente(ex: realizar uma reserva).

- ***Modem GSM:*** este possibilita que o sistema seja versátil do ponto de vista do cliente. Na realidade, este é responsável por enviar as referências de pagamento via SMS para o telemóvel do cliente a quando de uma reserva. Isto possibilita que um cliente ao se deslocar a um agente de pagamento não necessite de transportar um documento adicional com as respectivas referências de pagamento, tornando assim possível a troca de informações electronicamente.

- ***Servidor* Web*:*** é o principal responsável por publicar o website *Ticket-ID* na Internet, o que possibilita o seu acesso ao público em geral. O servidor *Web* também é um elemento chave do sistema de informação, uma vez que, o seu papel consiste em gerir correctamente os dados entre os diferentes elementos, de forma a que o fluxo da informação se processe automaticamente,rapidamente e sem anomalias.

5.1.2 Módulo do agente de pagamentos

Nesta secção apresenta-se o módulo do agente de pagamentos. O diagrama 5.3 mostra de forma simplificada as tecnologias envolvidas durante o processo de pagamento de um bilhete.

Figura 5.3: Diagrama com a arquitectura do agente de pagamentos.

Tendo em conta a descrição do sistema, após o cliente receber a SMS com a referência de pagamento este faz a respectiva liquidação apresentado paralelamente as suas credenciais pessoais. Concluído o pagamento, este recebe automaticamente um bilhete válido no telemóvel, via MMS no formato *QR-Code* ou via NFC.

Seguidamente apresentam-se as tecnologias utilizadas que permitem produzir no final o respectivo bilhete com as credenciais pessoais associadas.

- ***Leitor NFC:*** este permite receber as SMS do cliente com a respectiva referência de pagamento e enviar os bilhetes para o telemóvel do cliente.
- ***Ligação ao* Web Service*:*** o agente de pagamento estabelece a conexão ao *Web Service* sobretudo para obter informações acerca dos bilhetes reservados para um determinado evento, este suporta ainda a venda directa de bilhetes para qualquer evento.
  Importa referir que o envio das respectivas MMS com os bilhetes é realizado através da comunicação interna estabelecida com o modem de GSM.
- ***Leitor de smart cards:*** após a referência de pagamento ser considerada válida o próximo passo consiste em converter a respectiva reserva num bilhete válido. A

codificação e construção do bilhete consiste na associação dos dados do bilhete às credenciais do cartão do cidadão (cliente), como tal é necessário existir um leitor de cartões para permitir o acesso às respectivas credenciais(certificados).

- ***Unidade Criptográfica:*** após o acesso às credenciais do cartão de cidadão é necessário assinar digitalmente o respectivo bilhete. Deste modo, a unidade criptográfica pode ser vista como uma parte do sistema capaz de realizar de forma segura a construção do bilhete.

5.1.3 Módulo do comerciante

Finalmente, o módulo do comerciante consiste em concluir o ciclo de vida do bilhete, ou seja, este verifica a respectiva validade do bilhete segundo o método de validação pré-definido. Ainda assim, o processo de obtenção do bilhete pode ser realizado utilizando diferentes tecnologias o que tornam o sistema versátil e inovador.

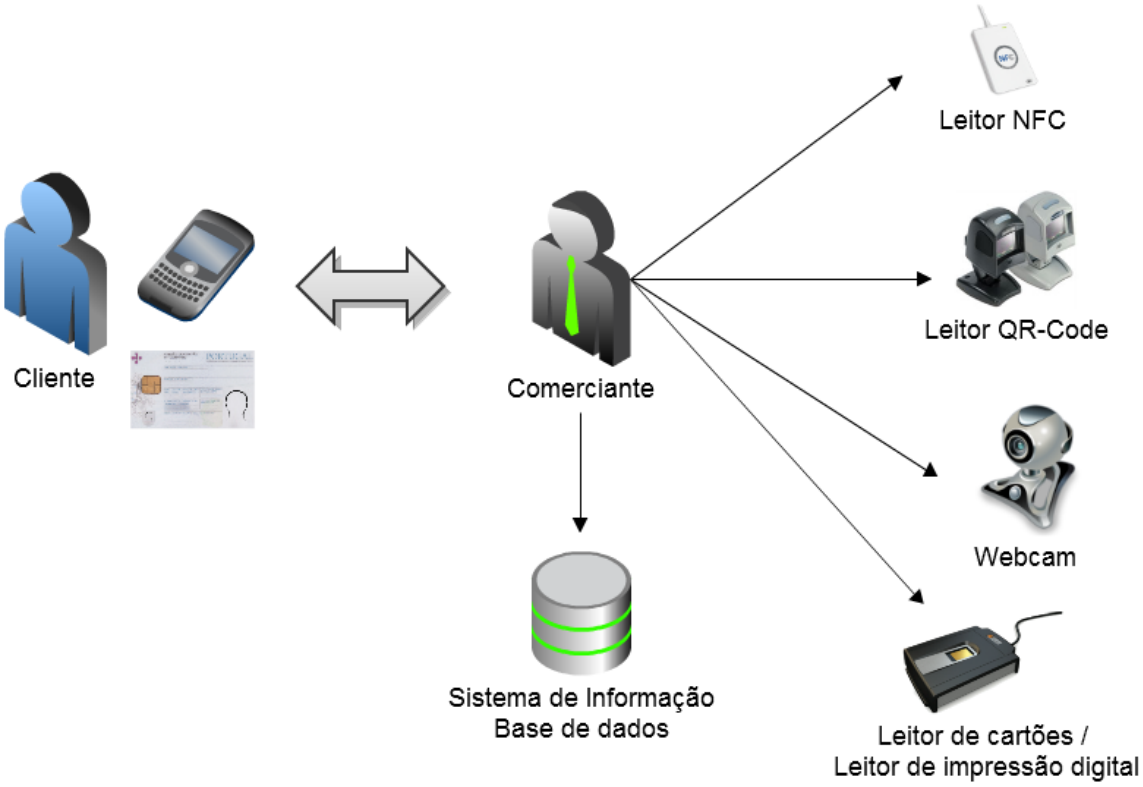

Figura 5.4: Diagrama com a arquitectura do comerciante.

O processo de validação é bastante simples, este consiste em que um cliente faculte ao comerciante o respectivo bilhete. Contudo, consoante o tipo de validação para o evento em questão pode ser necessário facultar ainda as credenciais do cartão de cidadão de forma a garantir a segurança do sistema e do cliente. Por isso, importa descrever todas as tecnologias utilizadas ao longo deste processo o que permite perceber as potencialidades associadas ao sistema.

- ***Leitor NFC:*** este é utilizado para obter a MMS do telemóvel do cliente com o respectivo bilhete.
- ***Leitor QR-Code:*** este leitor é utilizado como tecnologia alternativa ao NFC, na prática a sua função consiste em ler o respectivo *QR-Code* do visor do telemóvel do cliente de forma a obter o bilhete.
- ***WebCam:*** apresenta-se como uma outra alternativa, sendo esta uma solução de baixo custo capaz de reconhecer o *QR-Code* no visor do telemóvel. Contudo podem existir modelos de telemóveis que não são compatíveis. Ainda assim, o uso da *WebCam* apenas é recomendado para situações onde o comerciante não tem recursos financeiros para adquirir um leitor de códigos de barras 2D, salvaguardando por isso a competitividade entre comerciantes, ou simplesmente como alternativa a uma anomalia de um leitor.
- ***Leitor de cartões e impressão digital:*** a sua utilização deve-se a dois factores: em primeiro lugar o leitor de cartões é necessário para obter as credenciais do cartão de cidadão do cliente na reconstrução do bilhete (validação forte); em segundo lugar pode ser necessário auferir a titularidade do cartão ao seu portador no acto de validação do bilhete, deste modo é necessário recolher uma impressão digital do cliente e valida-la com a impressão digital armazenada no cartão de cidadão (*Match-On-Card*).
- ***Sistema de Informação - base de dados:*** o sistema de informação do comerciante armazena todos os bilhetes vendidos de cada evento.

5.2 Camada de Segurança

A arquitectura e o modo de funcionamento do sistema *Ticket-ID* é em alguns casos semelhante aos sistemas de bilhética actuais, estas semelhanças são mais patentes em relação ao sistema de informação. No entanto, o sistema desenvolvido faz a interligação de várias tecnologias, tais como, NFC, *QR-Code* e *smart cards* que associadas ao telemóvel permitem obter como resultado um sistema bastante inovador, original, prático e funcional.

Embora a nível tecnológico o sistema seja de facto inovador, este destaca-se sobretudo dos restantes sistemas devido à camada de segurança implementada. Isto é, enquanto que os sistemas similares (ex: Bilhética Transportes Públicos - OTLIS) centralizam a segurança do seu sistema na tecnologia (ex: Cartões RFID), por sua vez o sistema *Ticket-ID* baseia toda a segurança do sistema nas credenciais do cartão de cidadão, sendo por isso a prova de conceito do sistema.

Seguidamente apresentam-se alguns conceitos chave sobre os elementos de segurança utilizados, e por fim descreve-se a camada de segurança projectada para cada um dos módulos apresentados.

5.2.1 Conceitos-Chave: Elementos de Criptografia

Esta secção pretende sobretudo abordar alguns conceitos chave sobre os elementos de criptografia utilizados na implementação da camada de segurança do sistema.

5.2.1.1 Função de *Hash* - *MD5*

Uma função de *Hashing* consiste em gerar um código de tamanho fixo (designado de código de *Hash*) a partir de uma mensagem ou documento de qualquer tamanho. Uma mensagem resulta sempre no mesmo código de *Hash*, sendo que a probabilidade de duas mensagens diferentes resultarem no mesmo código é infinitesimal, o que faz do código único. Além de ser único é unidireccional, isto é, na prática é impossível reverter o código e determinar qual a informação que lhe deu origem [61] [8].

No que diz respeito aos algoritmos de *Hashing*, um dos mais utilizados actualmente é o MD5 (*Message-Digest algorithm 5*). Este tem um comprimento máximo de 128 bits e foi desenvolvido pela *RSA Data Security* , por exemplo, é muito utilizado em protocolos *P2P* e na verificação de *Logins*. Embora ultimamente este algoritmo tenha sido alvo de ataques por criptoanálise conhecidos[69]. Julga-se que no contexto em que é inserido no sistema *Ticket-ID* em pouco poderá afectar o mesmo, pois como se referiu anteriormente a segurança do sistema baseia-se nas credenciais do cartão de cidadão.

Prova desse facto é que a adição de um código de *Hash* a uma mensagem não garante a sua integridade, dado que tanto a mensagem como o respectivo código de *Hash* podem ser alterados posteriormente por terceiros. Assim, para que o código de *Hash* garanta a que a mensagem não foi alterada e o remetente da mesma é quem diz ser é necessário produzir-se uma assinatura digital (cartão de cidadão).

5.2.1.2 Assinatura digital - *SHA-1 e RSA*

A assinatura digital pode ser vista de forma análoga a uma assinatura manuscrita, mas neste caso aplicada a documentos digitais. Contudo, a implementação de uma assinatura digital é mais complexa do que assinar documentos em papel, uma vez que um documento digital pode ser facilmente alterado e copiado. Deste modo, uma assinatura digital deverá ser associável unicamente a uma entidade/pessoa e deve ser possível valida-la universalmente.

Assim, o processo de assinatura digital divide-se em duas partes, a primeira diz respeito à geração da assinatura e a segunda à verificação da assinatura.

- **Geração da assinatura:** em primeiro lugar, deve ser gerado um par de chaves pública/privada do signatário, seguidamente deve produzir-se uma sequência de bytes do documento digital (resumo - código de *Hash*) que se pretende assinar. Após ser gerado o respectivo código de *Hash*, deve-se cifrar o mesmo utilizando a chave privada do signatário, de forma a garantir a autenticidade, integridade e o não repúdio da mensagem que se pretende enviar. Como resultado deste processo criptográfico (ex: Sha1 e RSA) obtêm-se a assinatura digital.
  Dito isto, na criptografia assimétrica apenas o signatário tem acesso à sua chave privada e como tal a sua identidade está automaticamente associada à mensagem,

sendo que qualquer tipo de alteração da mensagem ou da assinatura é detectável.

- ***Verificação da assinatura:*** para se verificar a autenticidade do documento é necessário decifrar a assinatura digital usando a chave pública do signatário. Como resultado obtém-se novamente o código de *Hash* da mensagem original. Seguidamente deve ser calculado o código de *Hash* da mensagem recebida e posteriormente comparado com o respectivo código decifrado.
  Se forem iguais a mensagem é autêntica e está íntegra, caso contrário deve ser rejeitada uma vez que foi alterada ou o remetente não é quem afirma ser.

Em suma, o processo de geração e a respectiva verificação da assinatura pretende apenas garantir que quem assina uma mensagem é o individuo correspondente à identidade em causa. Por outro lado, a verificação da respectiva assinatura tem como objectivo garantir ao receptor da mensagem que a mesma não foi alterada e foi enviada por quem a assinou, neste caso o detentor da chave pública. Importa ainda referir que existem outros mecanismos para além da assinatura, por exemplo, o selo temporal que atesta o conceito de tempo à assinatura, os quais podem ser úteis na evolução da camada de segurança do sistema.

5.2.2 Mecanismos de Segurança da plataforma de venda

Em relação à plataforma de venda, em termos de segurança os servidores de base de dados, email, *Web Service*, GSM Modem e Web encontram-se instalados na mesma rede o que permite que a comunicação com o exterior sobretudo via Internet, seja possível de assegurar recorrendo aos métodos de segurança mais usados: *Firewalls*, *VPNs*, *Https*, *Ipsec*, entre outros.

5.2.3 Mecanismos de Segurança no agente de pagamento

No módulo do agente de pagamento a camada de segurança é mais exigente, pois é um elemento do sistema a funcionar num ambiente exterior (distribuídos pelo país). Assim, qualquer agente de pagamento associado ao sistema *Ticket-ID* deve ser autenticado e registado, o que implica cumprir os requisitos de segurança necessários ao bom funcionamento do sistema, tal como acontece actualmente nos agentes *PayShop* e nos comerciantes com terminais multibanco.

Deste modo, a ligação ao *WebService* do sistema deve ser salvaguardada mais uma vez pelos mecanismos de segurança habituais (*Https*, *VPNs*, *Ipsec*, *Firewalls*). Em relação à unidade criptográfica esta é responsável por efectuar a codificação do bilhete, como tal deve funcionar num ambiente controlado.

5.2.3.1 Processo de Venda de bilhetes

Tal como se referiu anteriormente, o agente de pagamento é o responsável por construir o bilhete, desta forma descreve-se todo o processo de codificação do mesmo, mais uma vez, é necessário salientar que será descrito o ciclo de vida completo do bilhete.

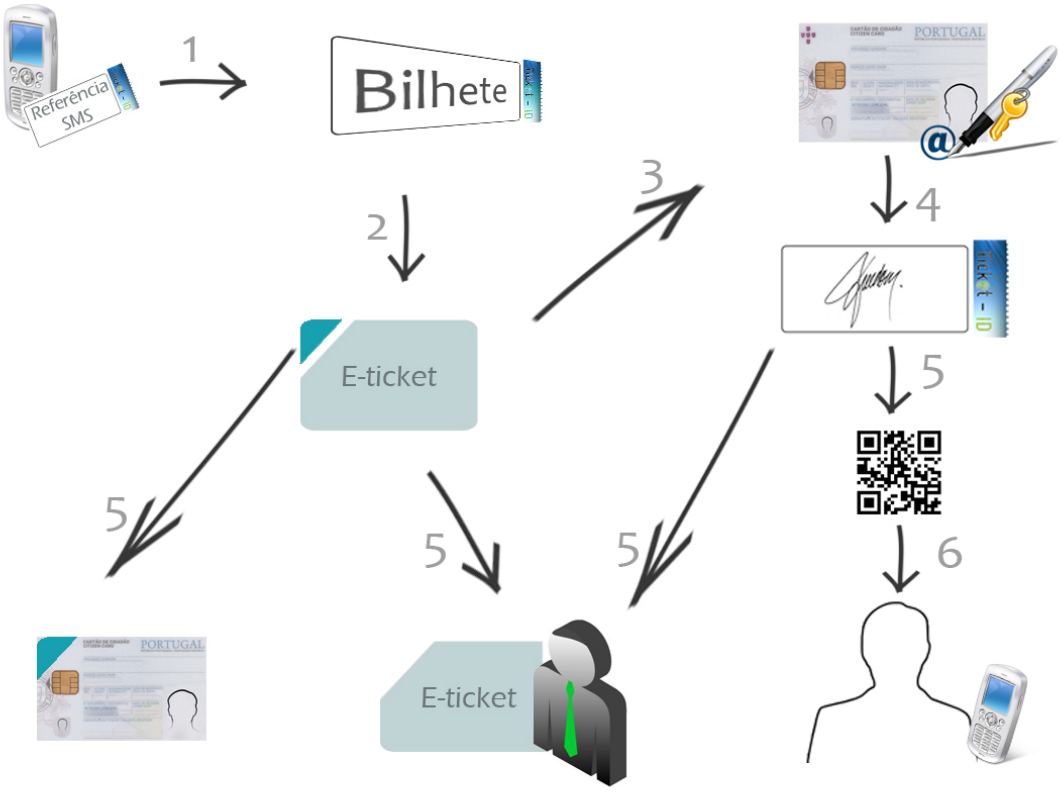

Figura 5.5: Diagrama do Processo de Compra.

1. O cliente desloca-se ao agente de pagamento e faculta através do telemóvel, via NFC, ou manualmente a referência de pagamento da reserva efectuada. O sistema ao iniciar a captura via NFC aguarda que o telemóvel lhe envie a informação do bilhete e os dados transmitidos, os quais contêm um identificador (*Ticket-ID*) caso contrário a leitura é cancelada.
   No caso de se utilizar um *smart card contactless* como portador do bilhete, substituindo o telemóvel NFC, este também terá de armazenar o respectivo identificador numa determinada área do cartão. Se no processo de leitura o acesso a essa área não contiver o respectivo identificador então é descartada a sua leitura.

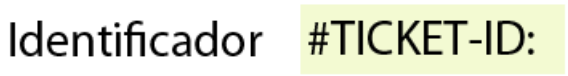

Figura 5.6: Identificador do bilhete no sistema.

2. Um bilhete no contexto do sistema é composto por vários elementos, nomeadamente pelos dados resultantes do pagamento e os respectivos detalhes do evento.

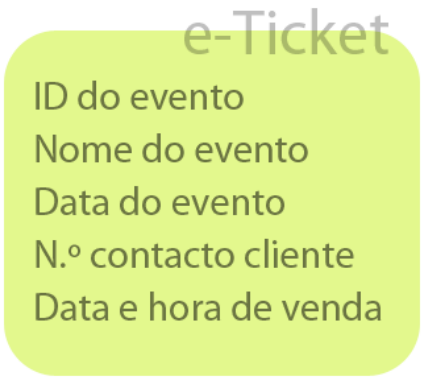

Figura 5.7: Ilustração dos detalhes do *e-Ticket*.

Após a construção do bilhete a unidade criptográfica do sistema aplica uma função de *Hash* (ex: MD5), a qual permite a transformação de uma grande quantidade de informação única e impossível de reverter, ao qual se deu o nome de ***e-Ticket***. Após a construção do *e-Ticket* é necessário associar as credenciais da identidade pessoal do cidadão ao respectivo bilhete e para isso é necessário assinar digitalmente (ex: SHA-1) o *e-Ticket*.

3. O processo de assinatura digital de um documento implica comunicar com o cartão de cidadão e para tal foi desenvolvido um novo *middleware* de raíz (ver capítulo 6) capaz de aceder a todas os dados do cartão e a outras funcionalidades que não estão disponíveis no *middleware* oficial (ex: Match on Card). O processo de assinatura do bilhete implica que o utilizador insira o código PIN da assinatura digital de forma a confirmar a operação.

4. O resultado da operação criptográfica anterior permite obter uma assinatura digital do *e-Ticket*, à qual se deu o nome de ***talão de controlo***. Nesta fase, o talão de controlo permite identificar inequivocamente o dono do bilhete.

5. Concluída a operação de emissão do talão de controlo, seguidamente efectuam-se três operações paralelamente. Em primeiro lugar o talão de controlo é armazenado no sistema de informação do comerciante, seguidamente o *e-Ticket* que deu origem ao talão de controlo é divido em duas partes de tamanhos diferentes:

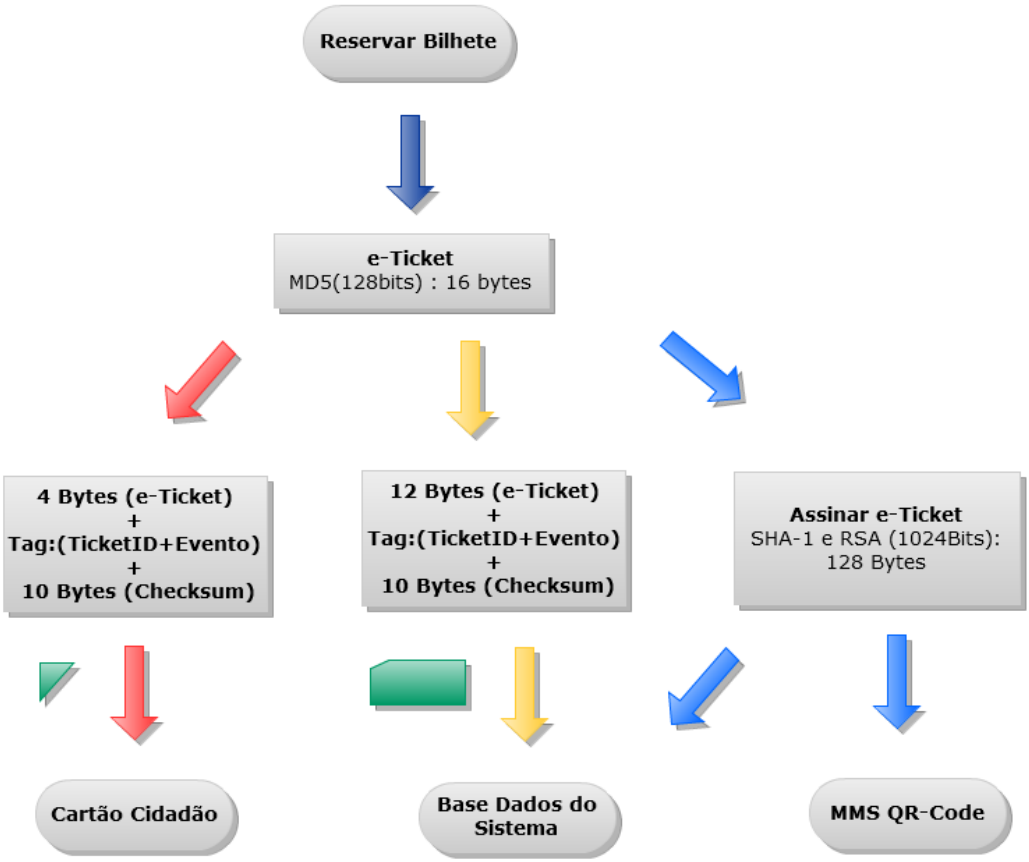

Figura 5.8: Fluxograma do Processo de Compra.

A parte mais pequena (a vermelho no diagrama 5.8) são os primeiros 4bytes do *e-Ticket* aos quais é adicionada um *tag* identificadora do bilhete e um *checksum* simples. A importância da tag identificadora baseia-se no facto de permitir ao cliente a posterior identificação do respectivo bilhete no seu cartão de cidadão. Em relação ao *checksum* este tem como função eliminar ambiguidades que possam existir em relação ao *e-Ticket* no cartão de cidadão.
Terminada a compilação desta parte, a mesma é colocada no cartão de cidadão na área reservada do cliente (1Kbyte) pelo agente de pagamento no acto de emissão do bilhete.

Em relação à área maior que compõe o *e-Ticket* (a amarelo no diagrama 5.8), esta é composta pelos restantes 12bytes aos quais também é adicionada a respectiva *tag* identificadora e o *checksum*. Por fim esta parte é enviada para o comerciante de forma a ser utilizada na autenticação forte.

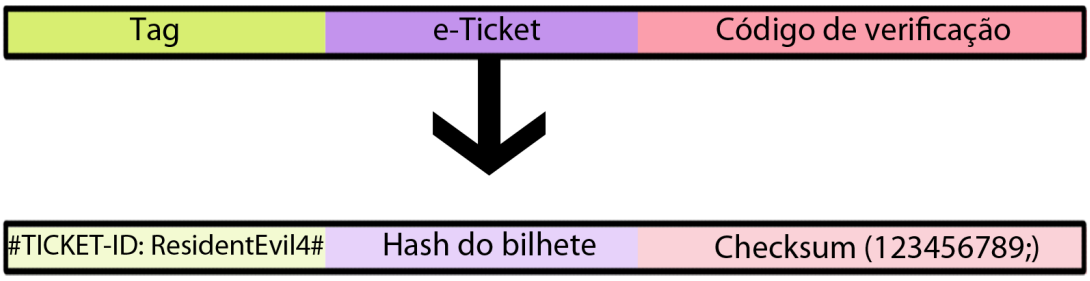

Figura 5.9: Exemplo de um *e-Ticket*.

6. Concluída a distribuição das pequenas partes do bilhete, é ainda necessário enviar para o telemóvel do cliente o talão de controlo que representa o bilhete na sua totalidade. Este processo implica codificar o bilhete no formato de código de barras 2D - *QR-Code*.

7. Por fim o agente de pagamento envia para o telemóvel do cliente uma MMS ou via NFC com o respectivo bilhete no formato *QR-Code*.

5.2.4 Mecanismos de Segurança do comerciante

O sistema do comerciante à semelhança do agente de pagamento, também é uma das partes integrantes do sistema *Ticket-ID* e como tal precisa de ser identificado e registado. Em termos de segurança definiram-se três métodos possíveis de validação dos bilhetes, devido ao facto de existirem ambientes que requerem outro tipo de autenticação mais forte.

5.2.4.1 Processo de Validação Simples

O processo de validação simples, consiste em descodificar a MMS através de uma das três tecnologias possíveis no lado do comerciante. Uma vez obtido o *talão de controlo*, a validação simples consiste em comparar apenas os talões de controlo, ou seja, o talão do cliente com o talão do comerciante armazenado no seu sistema de informação.

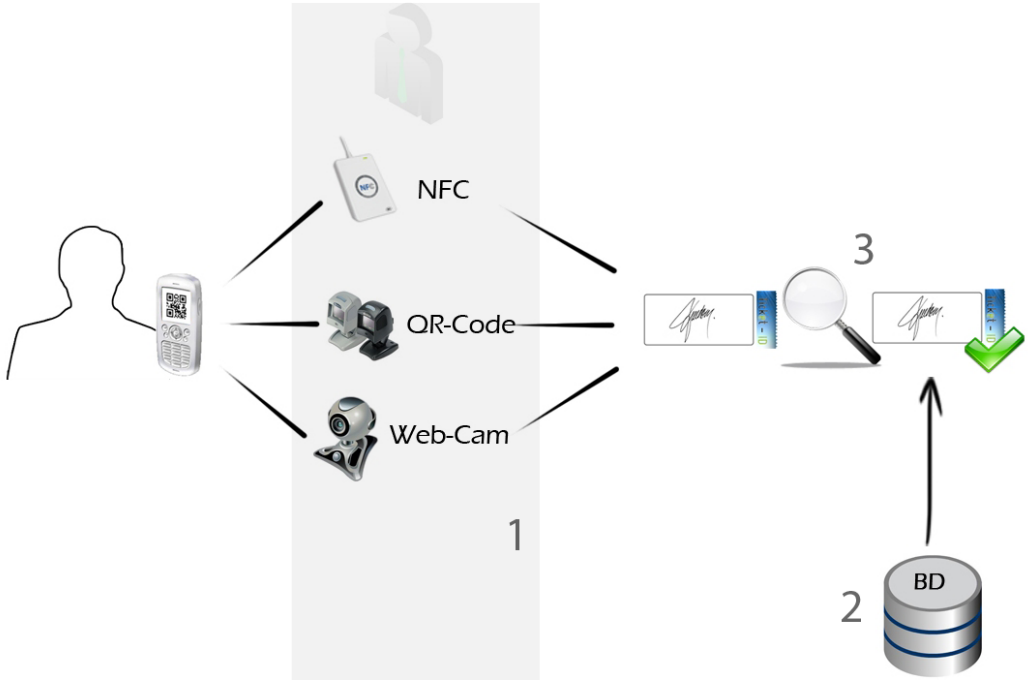

Figura 5.10: Diagrama do Processo de Validação Simples.

5.2.4.2 Processo de Validação Forte

À semelhança do processo de validação simples, em primeiro lugar é necessário obter e descodificar a MMS a partir de uma das tecnologias para obter o respectivo *talão de controlo*. O próximo passo consiste em validar os talões de controlo, mas neste caso (validação forte) o processo é algo diferente.
De seguida descrevem-se todas as fases do processo de validação forte:

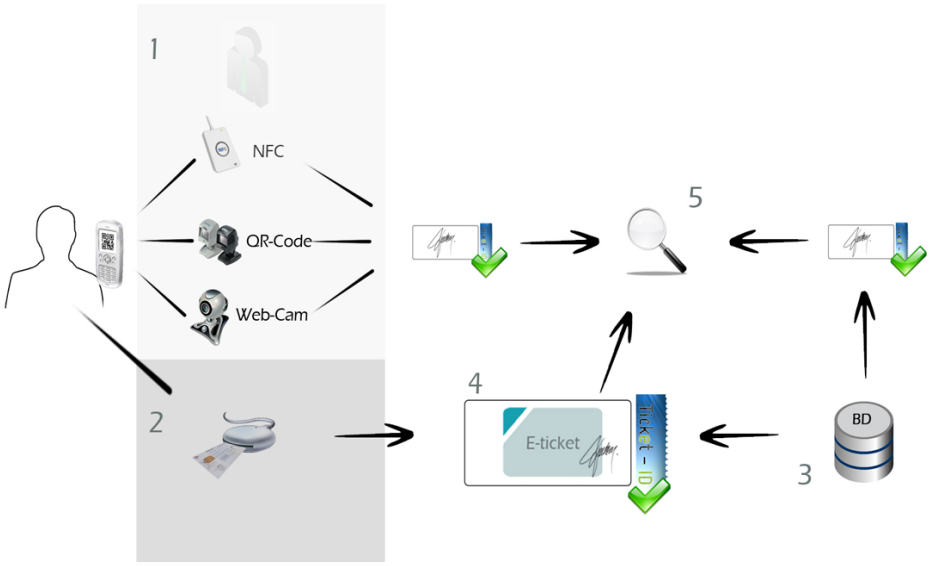

Figura 5.11: Diagrama do Processo de Validação Forte.

1. O comerciante possui um talão de controlo do bilhete completo e mais uma parte do *e-Ticket*($\frac{3}{4}$).

2. O consumidor em primeiro lugar coloca o seu cartão de cidadão no leitor do comerciante para facultar a outra parte do *e-Ticket*($\frac{1}{4}$) ao comerciante. Deste modo o comerciante obtém a totalidade do *e-Ticket*.

3. Após possuir o *e-Ticket* completo é agora necessário que o cliente coloque o PIN da assinatura do cartão para assinar digitalmente o ***e-Ticket***, permitindo assim a reconstrução do ***talão de controlo***.

4. Neste momento, é possível ao comerciante validar o bilhete. A validação consiste em comparar o *talão de controlo* reconstruído, com o talão armazenado no seu sistema de informação.

5. Caso seja necessário pode ainda ser requisitado o *talão de controlo* que o cliente recebeu no seu telemóvel, salvaguardando qualquer problema de segurança associado ao simples furto do cartão de cidadão. Assim, caso os três talões sejam iguais então o bilhete é válido.

5.2.4.3 Alternativa ao Processo de Validação Forte

Em ambientes sensíveis, por exemplo em aeroportos, também pode ser necessário auferir a titularidade do documento ao seu portador. Neste caso, para além de ser verificado o talão de controlo também é obrigatório identificar o cidadão que apresenta o cartão de cidadão, para isso recorre-se à validação biométrica da impressão digital armazenada no cartão de cidadão (processo de Match On Card). Este processo mais robusto permite provar que quem apresenta o cartão possui a identidade correspondente ao cartão e consequentemente é o dono do bilhete (assinatura digital).

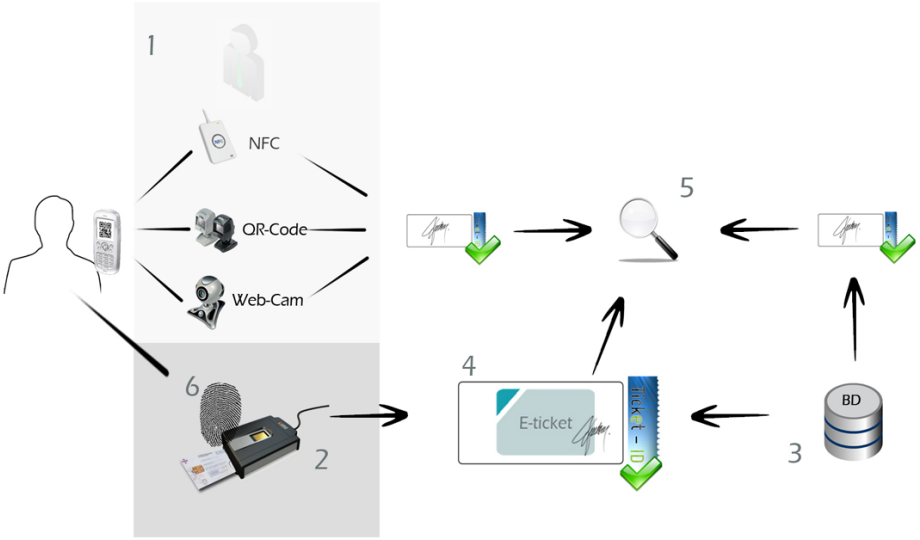

Figura 5.12: Diagrama do Processo de Validação Extra Forte.

Tal, como se pode observar, este processo de validação não acrescenta mais segurança do ponto de vista criptográfico, apenas permite auferir a titularidade do documento ao seu portador. No entanto, esta alternativa pode ser muito mais interessante no sentido de substituir a introdução do código PIN da assinatura, sendo que para isso será necessário uma nova investigação por forma a substituir-se a autorização do código PIN pelo reconhecimento da impressão digital.

5.3 Questões pertinentes

A presente secção expõe algumas questões sobre a implementação do sistema e sobre a camada de segurança do mesmo.

- O agente de pagamento ao ter conhecimento do código de *Hash* (*e-Ticket*), pode utilizar ou criar um bilhete (*talão de controlo*)?

  - O principal responsável por construir os *e-Ticket* é o agente de pagamento, contudo cada bilhete é construído no acto de venda com os dados relativos ao evento, à venda (ver 5.7) e com base nas credenciais do cartão de cidadão do cliente. Dito isto, a criação de um bilhete é praticamente impossível devido às credenciais estarem no cartão e sem elas não é possível criar um bilhete.

  Caso exista um ataque malicioso ao agente de pagamento este não armazena nenhum talão de controlo, isto é, o agente de pagamento apenas constrói os bilhetes e reencaminha-os para os destinatários (base de dados do sistema e para o cliente).

  Por outro lado, se for furtado o talão de controlo após o processo de criação do bilhete, o agente de pagamento fica comprometido e o atacante poderá utilizar o mesmo. Ainda que para isso seja necessário identificar no respectivo talão de controlo (assinatura digital) ou por engenharia social a que evento se destina, contudo este bilhete apenas é possível de ser utilizado em validações simples.

  Importa ainda referir que o agente de pagamento deve estar identificado e registado no sistema *Ticket-ID* para que cumpra os requisitos mínimos de segurança ao bom funcionamento do sistema.

- Uma vez que o cartão de cidadão armazena uma parte do *e-Ticket* como é feita a gestão do espaço no cartão de cidadão?

  - No acto de compra o agente de pagamento coloca o respectivo *e-Ticket* no cartão de cidadão. Na eventualidade de não existir espaço disponível no cartão então o processo fica em espera e o cliente terá que gerir o seu cartão de forma a ser possível armazenar o novo bilhete, uma vez que o espaço reservado no cartão de cidadão é da responsabilidade do cidadão.

- O que acontece se o cartão contiver outro tipo de informação? O cidadão pode aceder ao seu espaço reservado e perceber que bilhetes é que tem armazenados?

  - O cidadão quando acede à área pública do cartão consegue identificar perfeitamente os bilhetes, isto porque cada bilhete tem uma *tag identificadora* associada. Se existir lá outro tipo de informação, esta não sofre alterações permanecendo intacta em qualquer comunicação com o sistema *Ticket-ID*.

- Quais são as consequências do cidadão ou outra aplicação apagar o que está no espaço reservado do cartão?

  - A consequência imediata é o cidadão ficar impossibilitado de usar o bilhete numa autenticação forte, uma vez que este tipo de autenticação requer a utilização do cartão de cidadão. Neste caso o cidadão terá que dirigir-se a um agente de pagamento e fazer prova do talão de controlo para poder realizar novamente o processo criação de um novo *e-Ticket*. Seguidamente o cliente terá que o assinar para obter um novo talão de controlo, o qual será enviado para todos os intervenientes e paralelamente será colocado novamente a pequena parte do *e-Ticket* no cartão de cidadão.

- Porque é que o *e-Ticket* está no cartão de cidadão e não no telemóvel?

  - Caso fosse colocado o *e-Ticket* no telemóvel, em qualquer situação de furto do telemóvel automaticamente perdia-se o comprovativo (segredo).
  Por outro lado, o bilhete ao ser colocado e utilizado com as credenciais do cartão de cidadão torna-se intransmissível.

- Na eventualidade do telemóvel ser roubado o cliente perde o bilhete?

  - Nesta situação o cliente deve notificar um agente de pagamento, seguidamente o agente de pagamento pode modificar o processo de validação de simples para forte, o que implica de imediato a utilização do cartão de cidadão e nesse caso fica salvaguardado o bilhete.
  No pior dos cenários, caso seja roubado o cartão de cidadão e o telemóvel é necessário o atacante também saber o PIN da autenticação. Nesta situação

mais delicada o cliente ao fazer a denúncia do furto, o sistema modifica automaticamente o tipo de validação de forte para "extra forte", ou seja, requer a validação da impressão digital ao portador do cartão.

- Se o telemóvel ficar sem bateria o bilhete deixa de poder ser utilizado?

  - Existem diversas alternativas que permitem contornar este inevitável acontecimento, isto é, no caso do bilhete ter sido armazenado e transmitido via NFC para o telemóvel, então é possível utilizar o telemóvel sem bateria e transmitir na mesma o bilhete via NFC.
  Por outro lado, caso tenha sido enviado um *QR-Code* também é possível imprimir este para um papel de forma a salvaguardar uma situação destas, contudo o cliente pode sempre solicitar neste caso que o estado da validação se modifique para forte e neste caso o *QR-Code* pode ser substituído pelo cartão de cidadão simplesmente.

- O bilhete armazenado no telemóvel é possível de ser transmitido?

  - A análise que foi realizada na fase de inicial de definição do sistema pretendeu abranger o máximo de situações possíveis, mas possivelmente outras podem não ter sido abordadas. Esta situação é em particular muito importante, veja-se por exemplo, um cidadão compra um bilhete para um determinado evento (ex: concerto) o qual pretende oferecer à sua filha. Obviamente que a MMS (bilhete) no telemóvel pode ser transmitida para outro telemóvel, no entanto, apenas é possível de ser utilizada em situações de validação simples.

5.4 Conclusão

O presente capítulo demonstra claramente as potencialidades inovadoras do sistema e a originalidade dada pela utilização do cartão de cidadão através da assinatura digital. Em relação à camada de segurança importa realçar e descrever as potencialidades dos dois tipos de validação, assim:

- Estes dois tipos de validação permitem que o sistema seja flexível e se adapte segundo as necessidades de cada entidade e consoante o tipo de evento.
- O consumidor também poderá requerer que a validação seja forte e neste caso o comerciante deverá realizar a validação desse modo caso seja possível.
- No acto de validação simples a velocidade de validação é quase instantânea, característica que possibilita que o sistema seja inserido nos mais diversos eventos onde aspectos como a velocidade de processamento são tidos como um critério essencial.
- Em relação aos mecanismos de segurança associados aos sistemas de bilhética, tal como se referiu anteriormente o simples furto do telemóvel pode permitir que um atacante utilize o mesmo de forma fraudulenta. No entanto e tendo em conta que o talão de controlo é uma assinatura digital, é praticamente impossível o atacante saber onde o utilizar pela simples observação do bilhete. Por outro lado, nestas situações o cliente pode sempre requerer que o comerciante modifique o tipo de validação para o seu bilhete.
- O sistema também é seguro do ponto de vista de ataques mais complexos. Veja-se, por exemplo, uma situação extrema onde é roubado o telemóvel, o qual possui um bilhete de avião, e ainda o respectivo cartão de cidadão. Neste caso, o atacante até pode saber o PIN de assinatura e poderá ludibriar a validação forte, mas neste tipo de cenários normalmente é necessário realizar o processo de validação da titularidade do documento ao seu portador.
- O sucesso do sistema está dependente de muitos factores, mas sem dúvida que um dos factores mais relevantes é o que as pessoas pensam sobre a segurança. Nestes termos, a originalidade da inclusão do cartão de cidadão no sistema, desperta o interesse das pessoas neste novo sistema de bilhética associado à segurança oferecida pelo cartão de cidadão.

- A flexibilidade de existirem dois tipos de validação é muito vantajoso. Apresentam-se dois exemplos onde se podem verificar as potencialidades do sistema:
  - A validação forte pode ser muito útil para cenários como o Aeroporto. Neste caso para além de ser necessário possuir um talão de controlo também pode ser requerida a validação da titularidade do bilhete o que implica uma segurança máxima no acto de validação. A este cenário podem-se ainda associar os *hooligans*, os quais fariam parte de uma lista de pessoas não autorizadas a viajar e a adquirir bilhetes para eventos desportivos, e como tal não podiam assinar digitalmente qualquer bilhete o que os impede automaticamente de validarem qualquer bilhete na validação forte.
  - A validação simples é muito vantajosa em cenários onde é necessário validar rapidamente os bilhetes. Nestes casos o valor do bilhete é normalmente reduzido e como tal não é necessário existir uma segurança tão exigente. Por exemplo, o acesso aos transportes públicos ou a entrada em concertos, teatro e cinema não requerem uma segurança tão elevada.
- Por último, existe também a possibilidade de se reutilizar um bilhete. Por exemplo, nos transportes públicos é muito comum comprarem-se várias viagens para um bilhete único. Este tipo de funcionalidades também pode ser suportado pelo sistema.

Em suma, a camada de segurança do sistema é a prova de conceito desta dissertação. Ainda que associada à área da bilhética julga-se que a sua implementação em outras áreas e noutros contextos seja igualmente vantajosa, solucionando problemas e melhorando a segurança de muitos sistemas de informação.

Dito isto, importa referir que é graças à utilização original e inovadora proporcionada pelo cartão de cidadão que foi possível desenhar a camada de segurança do sistema, contudo para isso foi necessário um estudo exaustivo do cartão de cidadão. Dadas as necessidades do sistema em termos de segurança constatou-se que o *middleware* fornecido pelo estado português não disponibilizava o conjunto de funcionalidades necessárias, e como tal deste modo foi necessário realizar uma investigação profunda ao mesmo com o objectivo de se desenvolver um *middleware* completamente de raíz, o qual se apresenta no capítulo seguinte.

Capítulo 6

Desenvolvimento do novo *Middleware*

Neste capítulo, são descritas as motivações e os diversos objectivos definidos no desenvolvimento de um novo *middleware*. Apresenta-se ainda a metodologia e os respectivos resultados alcançados ao longo do processo de engenharia reversa sobre o cartão de cidadão.

6.1 Motivações e objectivos

As principais motivações que levaram ao desenvolvimento de um novo *middleware* foram as características e as funcionalidades que o projecto *Ticket-ID* contempla, mais concretamente o método/processo de *Match-On-Card* e o de assinatura digital.

Tendo em conta o facto da aplicação e o *middleware* disponibilizados pelo governo português não incluírem algumas funcionalidades essenciais ao desenvolvimento do projecto (ex: MoC). Contudo, tornar possíveis estas funcionalidades implica perceber e dominar o processo de comunicação com o cartão de cidadão, tarefa que não se revelou fácil devido à falta de informação pública.

Importa afirmar que apesar do *middleware* ser o principal elemento que permite a interacção com o cartão, julga-se que os detalhes técnicos que regem as comunicações com os *e-ID* deviam ser públicos, até porque o trabalho aqui descrito permite reconstrui-lo.

Definiu-se então como objectivo, realizar-se um processo de engenharia reversa sobre o cartão de cidadão com o intuito de obter os comandos que permitem obter informações e realizar operações a partir do cartão. Desta forma o sistema *Ticket-ID* pode contemplar o uso de novas funcionalidades e mais ainda, estas novas funcionalidades permitem que o sistema seja inovador e se destaque dos similares existentes no mercado.

6.2 Metodologia

Nesta secção, vamos começar por descrever o processo de reengenharia utilizado para o cartão de cidadão Português. O cartão de cidadão Português é um *smart card* e como tal é necessário entender os mecanismos de comunicação de baixo nível os (APDUS - secção 2.3.1.3) a fim de compreender como aceder aos dados e às funcionalidades instaladas no cartão (ex: realizar uma validação biométrica de um cidadão). O diagrama 6.1 ilustra a metodologia seguida que resulta num novo *middleware* que permite aceder a todas as funcionalidades descritas.

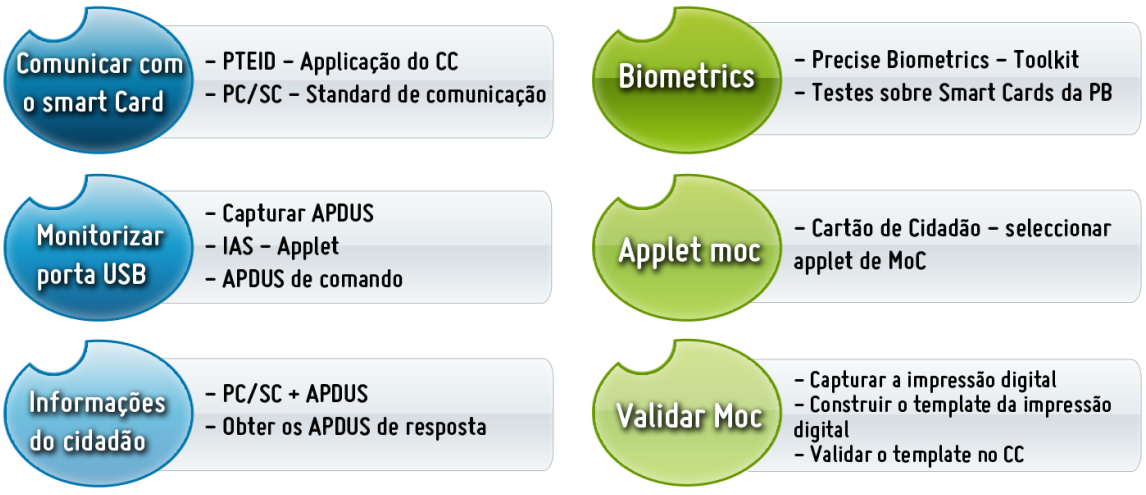

Figura 6.1: Ilustração da metodologia seguida.

Assim, em primeiro lugar optou-se por obter a informação dum cidadão utilizando a aplicação disponibilizada pelo governo português e em simultâneo monitorizou-se a porta USB a quando dessa comunicação. Deste modo, conseguiram-se obter os *APDUS* trocados entre o cartão de cidadão e a aplicação, o que tornou possível criar um novo *middleware* capaz de aceder aos dados do cidadão.

Em segundo lugar, sabendo que a *applet* instalada no cartão é da responsabilidade da *Precise Biometrics*, averiguaram-se as soluções disponibilizadas e efectuaram-se alguns testes em cartões de teste da *Precise Biometrics* com o objectivo de perceber como efectuar o MoC. O resultado alcançado nesta fase, permitiu que o mapeamento destes testes para o cartão de cidadão fosse praticamente imediato. Como resultado final, desenvolveu-se um novo *middleware* capaz de aceder às duas *applets* instalas no cartão de cidadão potenciando deste modo o acesso a novas funcionalidades.

6.3 Processo de Engenharia reversa - *Sniffer*

O programa utilizado para monitorizar a porta USB foi o *SniffUSB 2.0* [55]. O *SniffUSB* é um programa que analisa o protocolo USB, isto é, filtra todo o protocolo de comunicação entre o computador e um dispositivo USB (leitor de cartões), registando toda a comunicação entre ambos.

Deste modo, a sua utilização em programas de teste (no modo de depuração) permite capturar todos os dados trocados, mais precisamente os APDUS. Embora estes estejam naturalmente encapsulados dentro de pacotes USB é possível analisar e identificar claramente os dados pretendidos. Importa novamente referir que o *sniffer* foi utilizado enquanto se executou a aplicação fornecida pelo Governo Português disponível gratuitamente no website [53].

Seguidamente é necessário perceber e interpretar os dados recebidos, para isso utilizou-se como fonte de informação adicional o website [65]. Imediatamente perceberam-se qual os significados dos respectivos APDUS, sendo que o primeiro que foi encontrado consiste em seleccionar a *applet* IAS onde estão os dados pessoais do cidadão.

Uma vez seleccionada a *applet* o sistema operativo do cartão, aguarda que novos comandos sejam transmitidos. Nesta fase realizaram-se vários testes sobre os diferentes APDUS identificados que permitem seleccionar os dados do cidadão, sendo que no final, conseguiram-se ajustar os APDUS de forma a obter os dados públicos do cidadão.

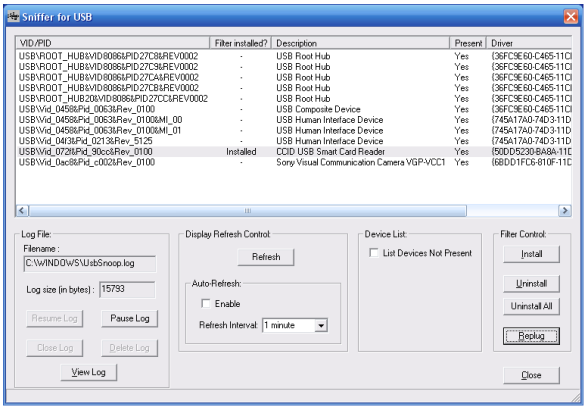

Figura 6.2: Programa *SniffUSB 2.0* .

6.3.1 *Wrapper* PC/SC

Identificados correctamente os APDUS necessários para estabelecer a comunicação com o cartão de cidadão, desenvolveu-se um *wrapper* através do standard PC/SC capaz de comunicar com o cartão de cidadão. Este *wrapper* permite o desenvolvimento de aplicações que comuniquem com o cartão de cidadão de forma independente (livre do *middleware* fornecido por terceiros, tais como o Governo Português). O *wrapper* é implementado como uma DLL que contém o código para criar e manipular as estruturas dos comandos APDU se têm de enviar e receber do cartão de cidadão.

Figura 6.3: Diagrama do *Wrapper* desenvolvido.

6.3.2 Middleware

Desenvolvido o *wrapper* que permite estabelecer a comunicação com o *smart card* através da norma PC/SC e enviar os APDUS necessários, realizou-se uma primeira comunicação com o cartão de cidadão de forma a testar o *wrapper* e os respectivos APDUS.
Quando se estabeleceu esta comunicação obteve-se o ATR do cartão.
O ATR é uma sequência de bytes que permitem definir as características da comunicação, tal como a velocidade de transmissão, o protocolo utilizado e o número de série do chip que possibilita identificar o tipo do cartão.

Obteve-se o seguinte *ATR*: **3B 95 95 40 FF D0 00 54 01 32.**

Uma pesquisa na Internet, no site [60], permite encontrar os *ATRs* de vários cartões conhecidos e facilmente se constata que o cartão de cidadão português também é contemplado nesta listagem, o que na prática significa que o *wrapper* identificou um cartão que de facto se trata do cartão português.

Estabelecida a comunicação com o cartão correctamente, é necessário seleccionar a *applet IAS* através dos APDUS descobertos pelo processo descrito. Após a selecção correcta da mesma, obtêm-se o código *"90 00"* no comando APDU de resposta enviado pelo cartão, o que significa que neste momento o sistema operativo do cartão está a executar a *applet* que armazena os dados pessoais.

A etapa seguinte é um pouco mais trabalhosa é necessário investigar a sequência de comandos APDUS transmitidos de forma a obter dos dados pessoais. No entanto, após realizados alguns testes, foi possível simplificar significativamente o número de comandos utilizados pela aplicação para capturar as informações necessárias.

As informações obtidas sobre o cidadão representam um total de *15,500 bytes*, mas é necessário converter estes dados no formato *UTF8* para ser possível de se apresentarem num formato legível. Esta fase é complexa, pois para além de ser necessário converter todas as informações é necessário fazer o particionamento do *buffer* de saída dos dados em diferentes blocos, onde cada bloco se refere a um elemento de informação (ex: nome).

Após a identificação de todos os dados públicos do cidadão decidiu-se também obter a fotografia do mesmo, uma vez que, esta se encontra nos *15,500bytes* de informação previamente obtida. Isto implica extrair correctamente a informação respeitante à imagem, dado que anteriormente quando convertemos os dados para *UTF8* facilitou a interpretação da informação obtida. Assim, é necessário apenas identificar no *buffer* dos dados, entre que bloco começa e termina a imagem.

A aquisição de dados da imagem e a sua posterior apresentação, à primeira vista é uma tarefa trivial. No entanto, muitas plataformas populares como *.Net* e bibliotecas *Java* padrão não suportam o formato *JPEG2000*, mas após uma cuidadosa pesquisa decidimos usar *CSJ2K - JPEG2000 Codec*, para a plataforma *.Net*. Esta ferramenta provou ser simples e funcional na construção e apresentação da imagem no formato pretendido.

Por último, obtidos todos os dados pessoais do cartão decidiu-se ainda aceder aos dados privados do cidadão, tais como a morada e o bloco de notas. Importa referir que em ambos os casos é necessário inserir o PIN correspondente de acesso aos dados. Realizando uma primeira análise, a inserção do PIN pode de facto ser um problema no acesso aos dados, mas na realidade é a chave da resolução do problema.

Tal como foi referido anteriormente, o processo de monitorizar a porta usb permite identificar os APDUS necessário para obter os dados. Neste caso, identificamos que o APDU que envia um PIN têm um formato especifico [65] e como tal a análise torna-se simples, ou seja, encontrando o APDU especifico de envio do PIN têm-se a sequência necessária de APDUS necessários para obter a morada, modificar o bloco de notas ou até mesmo assinar um documento digitalmente, uma vez que todas estas funcionalidades necessitam da inserção de um PIN.

6.3.3 Resultados

Como resultado desta metodologia, utilizou-se o *middleware* para se desenvolver uma aplicação que contém vários aspectos similares à aplicação do Governo Português. A aplicação desenvolvida é capaz de obter os dados públicos e privados do cidadão,

manipular o bloco de notas pessoais e ainda instalar os certificados pessoais no *KeyStore* do *Windows*.

Apresenta ainda como grande vantagem a possibilidade de assinar digitalmente qualquer documento e realizar a respectiva verificação da assinatura directamente no cartão ou através dos certificados pessoais instalados no *Windows*. Esta funcionalidade não é fornecida por qualquer aplicação oficial, embora o processo de assinatura de documentos em *Adobe Acrobat* e *Microsoft Office* é descrito nos manuais de utilizador facultados no site do cartão do cidadão.

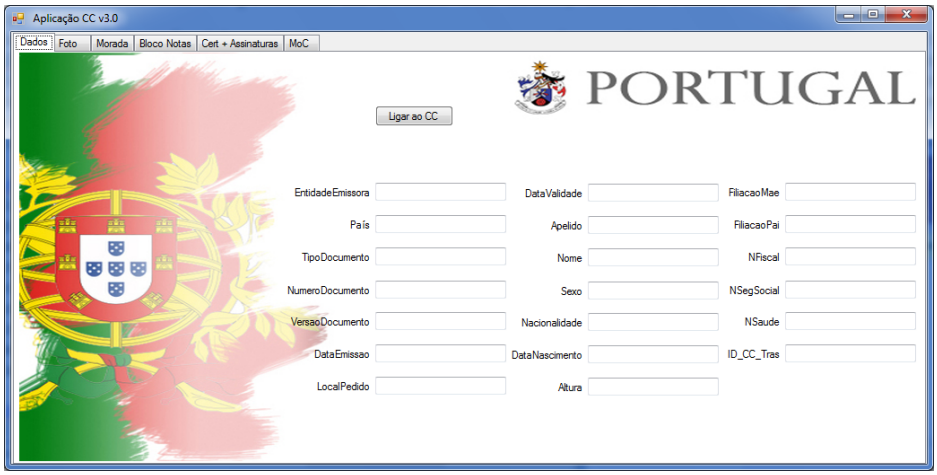

Figura 6.4: Aplicação que utiliza o *middleware* desenvolvido.

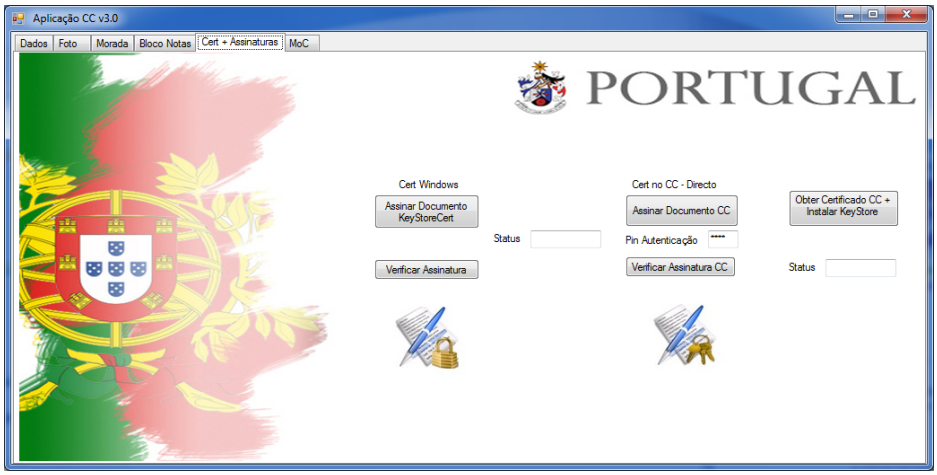

Figura 6.5: Aplicação - Assinar digitalmente documentos.

6.4 Processo de Engenharia reversa - *MoC*

A segunda parte da metodologia consiste em realizar a operação de validação biométrica de um cidadão, método vulgarmente conhecido de *Match-on-Card* (MOC). Importa referir que este deve ser sempre realizado num ambiente controlado de forma a garantir que os dados biométricos extraídos pertencem ao indivíduo a que se pretendem auferir a titularidade do documento.

Dito isto, esta segunda fase do processo de reengenharia implica em primeiro lugar seleccionar a *applet* de MoC com a finalidade de posteriormente enviar os comandos APDUS necessários para realizar o processo. A selecção da *applet* é simples pois em relação à *applet IAS* apenas muda um byte no comando APDU de selecção. Em relação aos APDUS necessários para realizar o processo, realizaram-se vários testes numa primeira fase em cartão de testes da *Precise Biometrics* usando um *toolkit* desenvolvido por eles para esse efeito.

Paralelamente, investigou-se o processo de comunicação, mais uma vez através do *sniffer*, entre este *toolkit* e o cartão da *Precise Biometrics*. E como resultado obtiveram-se os APDUS necessários que devem ser transmitidos, exploraram-se assim os mesmos no cartão de cidadão e o processo foi satisfatório.

6.4.1 Modelo de dados da Impressão Digital - (*template*)

A quando da emissão do cartão de cidadão, é realizado o processo de aquisição da impressão digital do cidadão. Este processo consiste em obter uma imagem de um dedo que é convertida num *template* com as minúcias da impressão digital, sendo posteriormente armazenado no cartão a quando da sua concepção.

Tendo isto em conta, então significa que o processo de validação (MoC) consiste enviarem os comandos APDUS correctos, sendo que nesses comandos deve ser enviado um *template* da imagem capturada da impressão digital de forma a este ser validado contra o *template* armazenado no cartão de cidadão (tarefa realizada pelo toolkit).

Deste modo, um *template* consiste na associação entre os dados de referência e um cabeçalho biométrico. O cabeçalho biométrico contém as informações relevantes para o tipo e forma dos dados exigidos pelo cartão e, portanto, são armazenados numa área pública do cartão. Porém, os dados de referência são armazenados numa área privada do CC e é esta que executa a verificação dos dados submetidos para validação. Um aspecto importante de segurança é que estes dados não podem ser extraídos nem alterados. A construção de um *template* da impressão digital consiste num algoritmo capaz de identificar uma série de cristas e vales, onde as cristas são pontos de minúcia, e onde termina uma crista existem bifurcações denominados vales que unem umas cristas a outras. Assim após a localização dos pontos de minúcia da imagem são armazenadas as posições e seguidamente é construído um modelo de dados (*template*).

Na fase de autenticação, a imagem da impressão digital adquirida é pré-processada e são extraídas as minúcias para criar um novo modelo (*template*) capaz de ser comparado com o modelo registado no cartão de cidadão. O processo de comparação consiste em tentar encontrar o maior número de pontos semelhantes, sendo que o resultado da correspondência entre ambos é geralmente o número de minúcias correspondentes.

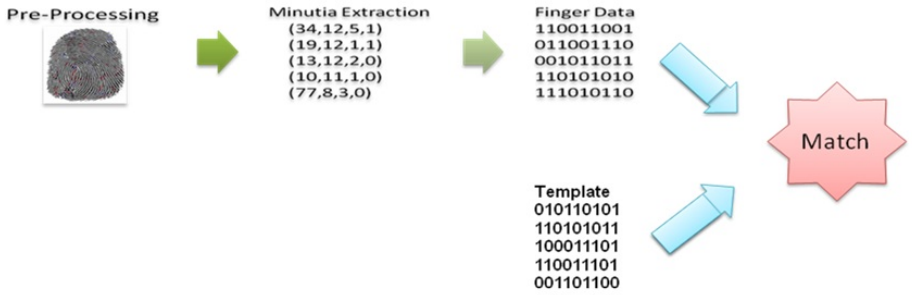

Figura 6.6: Ilustração da construção de um *template*.

6.4.2 Realizar *MoC*

Assim, neste contexto para se validar um *template* é necessário primeiro construí-lo, para isso é necessário primeiro capturar a impressão digital e seguidamente construir o *template*. Contudo é necessário possuir um algoritmo capaz de identificar os pontos de extracção e construir o respectivo modelo de dados.

Neste passo decidiu-se utilizar o *toolkit* da *Precise Biometrics* para construir o *template*, uma que o *template* instalado no cartão de cidadão é possível de ser validado contra os *templates* criados por este.

Neste contexto, tendo em conta o objectivo de realização do MoC no cartão, utilizou-se o *toolkit* para realizar a captura da imagem e construir o *template*. Após a construção do *template* este é enviado através dos APDUS identificados e no final verifica-se a validade da impressão digital, caso seja então o código devolvido pelo cartão é o *"90 00"*, o que significa que a pessoa é a mesma que apresenta o documento.

6.4.3 Resultados

Considerando todos os passos desenvolvidos ao longo do processo de reengenharia, obteve-se como resultado um novo *middleware*. Como tal, considerou-se desenvolver uma outra aplicação que o utilizasse de forma a testar todas as funcionalidades investigadas antes de ser usado no sistema *Ticket-ID*.

Assim a aplicação desenvolvida captura os dados do cartão de cidadão e possibilita ainda a utilização da funcionalidade de MoC esta foi desenvolvida na plataforma *.Net* e apresenta características bastante interessantes. Mais uma vez importa recordar que esta foi projectada de acordo com as necessidades do sistema *Ticket-ID* onde é necessário auferir a titularidade ao portador do cartão.

Figura 6.7: Aplicação/Protótipo desenvolvido para realizar o MoC.

Descrevem-se de seguida algumas das principais características da aplicação que esta disponível para consulta na Internet em, *http://cc.di.ubi.pt* :

- Detecção automática de inserção e remoção do cartão.
- Uma animação que representa a leitura dos dados do cartão.
- Apresentação gráfica dos dados dos cidadãos, incluindo uma foto animada.
- O feedback da autenticação via MoC, consiste em manipular a imagem da impressão digital(cinza/preto) para a cor verde ou vermelha respectivamente.
- São emitidos também sons intuitivos capazes de indicar a autenticação satisfatória ou não.

6.5 Conclusão

Por fim, importa ainda referir que o "road map"(metodologia) permitiu o desenvolvimento de um novo *middleware* e consequentemente o acesso a novas funcionalidades do cartão de cidadão. Esta metodologia também foi utilizada e com sucesso na construção de um *middleware* capaz comunicar e armazenar informações em cartões NFC utilizados no contexto do sistema *Ticket-ID*. Muito embora neste caso o fabricante do cartão disponibilize mais documentação e informação sobre os cartões *MiFare*.

Em suma, o objectivo de desenvolver um novo *middleware* para o cartão de cidadão foi alcançado e provou-se ainda que a metodologia seguida foi a adequada dado que permitiu obter o mesmo sucesso com os cartões NFC.

Capítulo 7

Implementação do sistema *Ticket-ID*

O presente capítulo descreve o sistema *Ticket-ID* do ponto de vista da engenharia de software. Apresentam-se os desafios de engenharia de software inerentes a cada um dos módulos do sistema, os quais são detalhados com a máxima precisão, permitindo uma interpretação intuitiva das funcionalidades desenvolvidas.

7.1 Metodologia de desenvolvimento do software

Como é conhecido o desenvolvimento de um software passa por diversas fases, as quais no seu conjunto reúnem actividades que têm como objectivo o desenvolvimento de um sistema de informação. Contudo, é necessário encontrar as melhores respostas para os diferentes desafios que surgem num projecto de engenharia de software. Assim, do ponto de vista do sistema *Ticket-ID* definiram-se quatro grandes desafios:

- **Heterogeneidade**: O sistema, de um modo global, dá respostas aos diversos ambientes tecnológicos e de execução heterogéneos, na medida em que lida com diferentes tecnologias (código barras, *smart cards*, etc).
- **Rapidez**: Um dos maiores desafios e exigência do mercado é a rapidez de processamento dos dados e de entrega do produto final ao cliente. Nestes termos o sistema ao ser desenvolvido em pequenos módulos permite automatizar ao máximo o tempo de execução, desenvolvimento e manutenção do sistema em cada uma das fases.

- **Usabilidade**: Tal como qualquer sistema de informação o seu sucesso está em muito dependente da confiança dos utilizadores. Como tal o sistema foi totalmente projectado de forma a que a sua usabilidade seja simples e intuitiva, de forma a não deixar dúvidas, incertezas ou desconfianças por parte do utilizador final.

- **Segurança**: O maior desafio de todos e que deve sempre ser tido em consideração no desenvolvimento de um software é a segurança, pois mesmo que um software responda a todas as necessidades e funcionalidades mas não apresente a segurança ideal, este rapidamente se transforma num fracasso. Assim, do ponto de vista da interacção do cliente com o sistema *Ticket-ID*, a utilização do cartão de cidadão potencia os melhores mecanismos de segurança e de confiança do sistema.

No que diz respeito, ao modelo de desenvolvimento utilizou-se o Cascate [68]. A escolha deste modelo deveu-se ao facto de se tratar de um modelo bastante específico, que permite que apenas se passe a uma nova fase de desenvolvimento assim que a fase anterior esteja concluída. Contudo, se necessário, é possível voltar a uma fase anterior para redefinir algo.

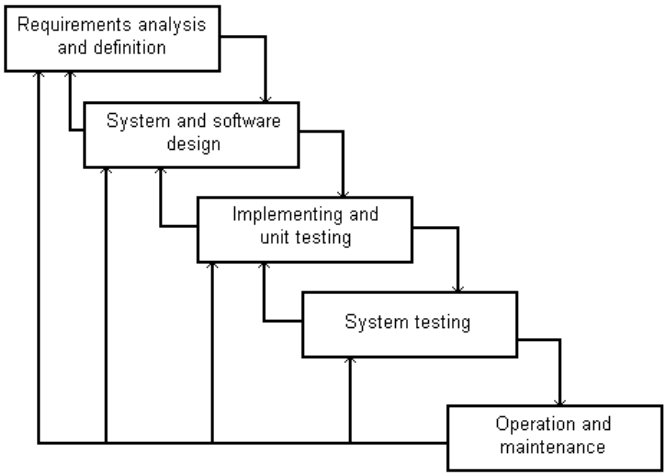

Figura 7.1: Ilustração do modelo de desenvolvimento de software seguido - *Cascate*.

7.2 Descrição dos componentes do sistema

7.2.1 Modelo de Base de Dados

Apresenta-se de seguida o modelo entidade-relação (nível conceptual) e o modelo relacional (nível lógico) que representam a base de todas as informações do sistema *Ticket-ID*. Importa referir que a base de dados desenvolvida suporta todos os módulos do sistema, os quais são descritos nas próximas secções.

- **Modelo E-R(nível conceptual):** O modelo de entidade-relação ilustra conceptualmente as relações entre entidades de bases de dados com alto nível de abstracção.

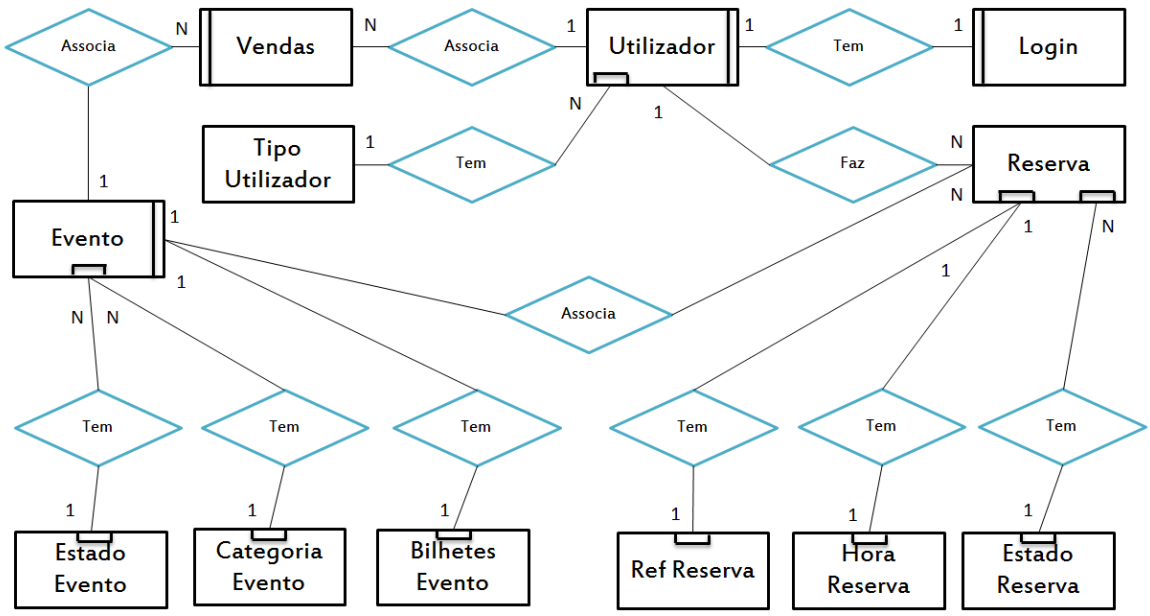

Figura 7.2: Sistema *Ticket-ID*: Modelo E-R.

- **Modelo Relacional(nível lógico):** apresenta-se na figura seguinte o M-R do projecto desenvolvido.

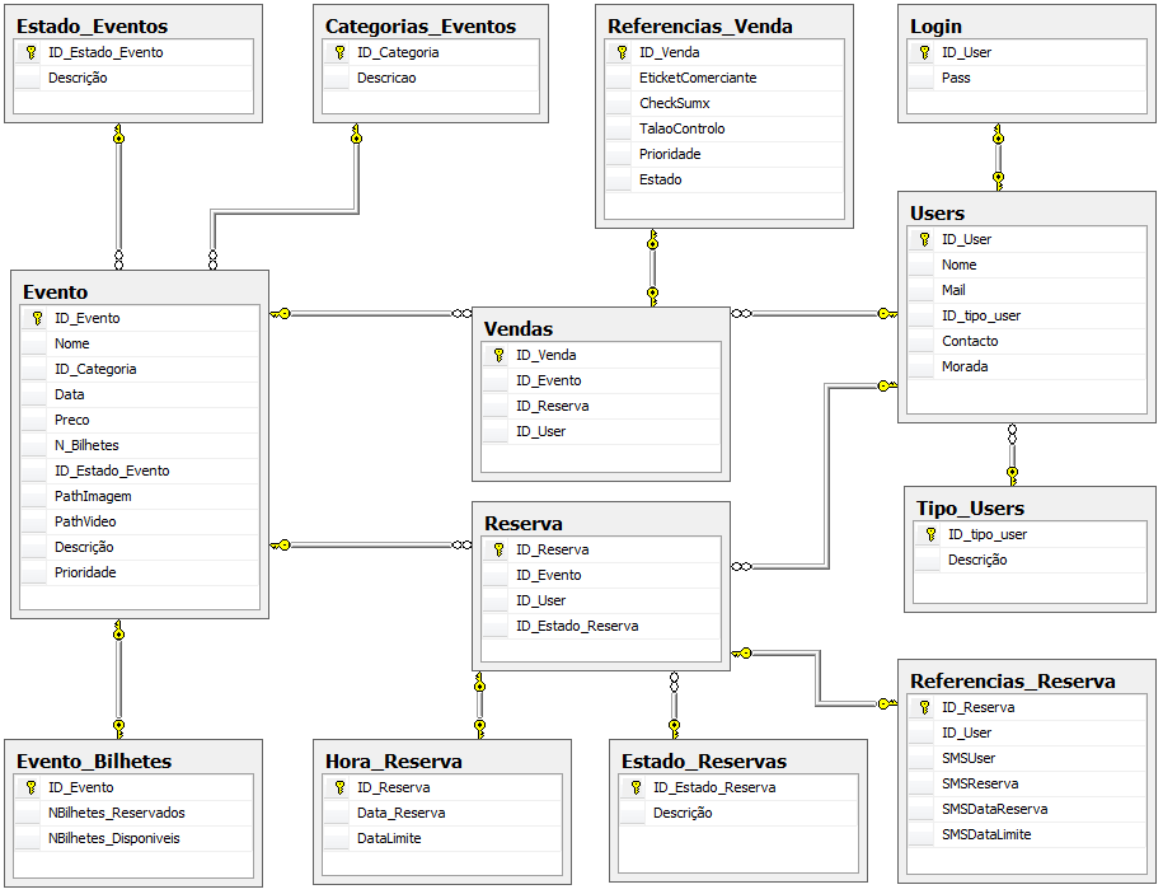

Figura 7.3: Modelo relacional - Diagrama da Base de dados.

No que diz respeito à BD desenvolvida, foram criados um conjunto de procedimentos que permitem a comunicação com a mesma para as mais diversas funcionalidades. Destacam-se por exemplo os procedimentos que permitem realizar uma nova reserva e o processo de venda.

- **Procedimento de Reserva:** este é responsável por efectuar uma nova reserva para um evento seleccionado no website pelo utilizador. Contudo, apenas permite que se realizem novas reservas oito horas antes do começo do evento.

- **Procedimento de Venda:** : o pagamento de uma reserva tem uma duração limite, deste modo, um pagamento deve ser realizado consoante o tipo de reserva escolhido. Caso receba a reserva por SMS o utilizador tem cinco horas para realizar o respectivo pagamento, no caso de não receber por SMS, mas apenas por email, o utilizador dispõe de duas horas para realizar o pagamento. Em suma, no acto de venda são verificadas estas regras e caso alguma falhe serão tomadas as devidas acções e actualizados os dados.

Por outro lado, devido às características temporais do sistema, em relação a reservas e vendas é necessário que a BD tenha mecanismos inteligentes associados capazes de as gerir. Tendo em conta este propósito desenvolveram-se procedimentos temporais (chamados *jobs* no SQL Server) capazes de garantir a veracidade e actualização dos dados em tempo real. Apresentam-se de seguida dois exemplos:

- *Valida Bilhetes:* O *job* valida bilhetes é executado de minuto a minuto e realiza as seguintes operações:
  - Selecciona todas as reservas no estado activo;
  - Vê a data limite de pagamento das reservas activas;
  - Efectua o teste com a hora do sistema e com a data limite de pagamento;
  - No caso do teste falhar, muda automaticamente o estado da reserva para cancelado e actualiza o número de bilhetes reservados e disponíveis.

- *Valida Evento:* Foi ainda desenvolvido um *job* que gere os estados dos eventos. Na prática este *job* é o principal responsável por toda a gestão dinâmica dos eventos no website. Apresentam-se as operações que este executa:
  - Encontra todos os eventos activos;
  - Verifica data do evento e testa com a hora do sistema;
  - Caso a validação falhe, muda o estado do evento para terminado e actualiza o número de bilhetes disponíveis para zero e o estado de todas as reservas desse evento para cancelado (caso ainda activas).

7.2.2 Módulo da Plataforma Web de Reservas

Realizada a descrição do modelo de base de dados que suporta todo o sistema, faz agora sentido descrever os módulos desenvolvidos. Deste modo, a plataforma de reservas é composta por uma página *Web* desenvolvida em *Silverlight* e em *Aspx .Net*, nesta página o utilizador pode realizar inúmeras operações. Apresentam-se algumas imagens da página desenvolvida e das respectivas funcionalidades.

7.2.2.1 Página Principal

Tal como se pode observar na figura 7.4, existe uma barra com diferentes botões (Info, Eventos, Conta Cliente, Cartão Cidadão, Suporte e Registar) onde cada um deles permite aceder a uma nova funcionalidade.
É possível ainda utilizar a barra de pesquisa de eventos para encontrar um evento específico. Por fim nesta barra, existe ainda o botão do carrinho de compras que é dinâmico e permite visualizar os eventos reservado, e ainda o botão da casa (*home*) que possibilita voltar à página incial.

Figura 7.4: Página Inicial: *Ticket-ID*.

Analisada a barra de menus importa ainda referir um aspecto interessante desta página inicial. No lado esquerdo da página encontra-se um calendário onde os dias dos espectáculos aparecem com uma cor diferente, e assim que seleccionados surge

um novo menu informativo sobre o dia seleccionado e os respectivos eventos para esse mesmo dia.

Finalmente, no centro da página encontra-se um conjunto de imagens dinâmicas em carrossel com os próximos eventos. Estes são carregados de forma dinâmica, isto é, colocam-se os eventos em destaque que acontecerão brevemente. É ainda possível ao utilizador passar o rato sobre a imagem e visualizar os detalhes do evento. De forma a centralizar ao máximo a informação sobre um evento é ainda possível visualizar um vídeo sobre o evento clicando apenas sobre a imagem, o que do ponto de vista do utilizador se torna mais intuitivo.

7.2.2.2 Página Principal - Login

Importa ainda referir que na página principal é possível realizar o login de um utilizador, uma vez que existem três tipos de utilizadores (normal, administrador, comerciante) permitindo assim aceder a novas opções e menus que ficam disponíveis na barra de opções.

Além de novas opções o utilizador ao realizar o login no sistema fica salvaguardado por mecanismos de segurança sobre a sua sessão, tais como, o facto da sessão expirar ao fim de cinco minutos de inactividade na página.

Figura 7.5: Página Inicial - Login.

7.2.2.3 Menu - Info

A primeira opção do menu é a "Info", uma abreviatura de informações. Neste menu, o utilizador poderá visualizar informações cruciais de forma a entender o real funcionamento do sistema em todas as suas fases.

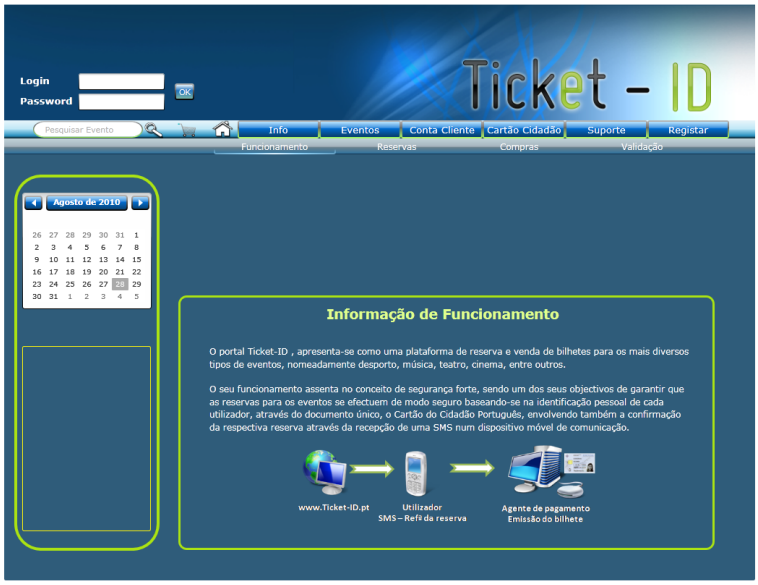

Figura 7.6: Menu Informações.

7.2.2.4 Menu - Eventos

No menu "Eventos", o utilizador dispõem de três opções - Agenda, Destaques, Inserir Eventos e Histórico. Assim, no que diz respeito à agenda a página é mais uma vez dinâmica (figura 7.7), ou seja, internamente é calculado o evento mais próximo e automaticamente é seleccionado e representado graficamente, sendo que pode ser escolhido outro qualquer.

Por sua vez, o menu destaque permite que sejam escolhidos os destaques por categoria. Tal como se pode observar na figura 7.8, o utilizador tem uma lista de categorias de eventos que poderá seleccionar. Seguidamente é apresentada uma tabela com todos os eventos para a selecção pretendida, a partir desta tabela é possível ao utilizador visualizar os eventos do seu interesse e reservar bilhetes para os mesmos.

Figura 7.7: Menu Eventos - Agenda.

Figura 7.8: Menu Eventos - Destaques.

É ainda possível ao administrador do sistema ou ao comerciante, inserir novos eventos no sistema. A imagem 7.9 mostra o menu onde são introduzidos os dados relativos ao novo evento que se pretende inserir, nomeadamente, a data, nome, hora, imagem publicitária, vídeo e outros. É de realçar ainda que é neste menu, no campo de validação, que o administrador/comerciante definem o tipo de validação do respectivo evento.

Figura 7.9: Menu Eventos - Inserir novo Eevento.

Por último, a opção de histórico é em tudo idêntico à opção de destaques com a simples diferença de serem apresentados apenas os eventos terminados. Na prática, esta opção é meramente informativa.

7.2.2.5 Menu - Conta

O menu "Conta", apenas está disponível quando o utilizador realiza o login, caso contrário tem apenas disponível a opção de recuperar a passowrd.
Assim, após realizar o login é possível manipular várias opções sobre a sua conta pessoal, como por exemplo, receber a SMS de reserva de bilhetes ou não.

É ainda neste menu que se localiza a opção mais importante, aquela que permite terminar um reserva ou simplesmente escolher os itens a reservar.
Tal como se observa da figura 7.11, é disponibilizada uma tabela ao utilizador com todos os itens que foram previamente seleccionados e se desejam reservar. No caso, de se pretender reservar de facto bilhetes para esses eventos, clica-se no botão finalizar deste menu e automaticamente recebe-se no email e no telemóvel uma mensagem com os detalhes da reserva.

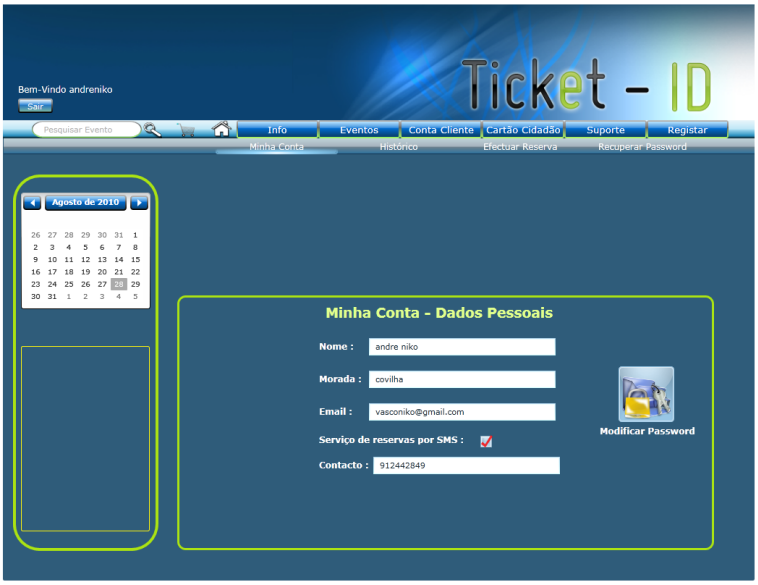

Figura 7.10: Menu Conta.

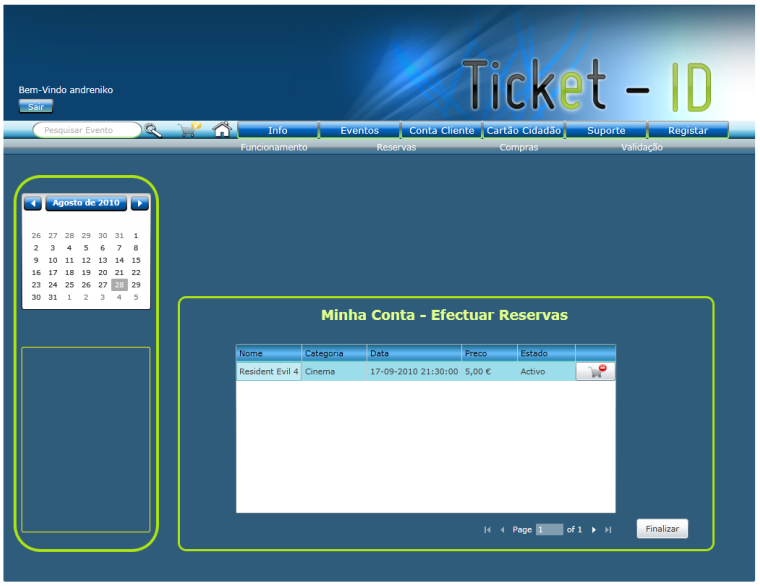

Figura 7.11: Menu Conta - Reservas.

7.2.2.6 Menu - Cartão de Cidadão

No que diz respeito ao menu do "Cartão do Cidadão", este é sem duvida bastante inovador. Na prática, é possível que o utilizador interaja usando o seu cartão de cidadão através do sistema pelo website. É assim possível ao utilizador consultar e gerir os seus bilhetes armazenados no cartão de cidadão. Importa referir que esta funcionalidade é de inteira responsabilidade do utilizador, devido ao facto de qualquer

alteração no bloco de notas do cartão de cidadão ser privado/protegido.

Como se observa na figura 7.12, o utilizador ao interagir com o seu cartão de cidadão no website, são recolhidos todos os bilhetes guardados no cartão, qualquer informação pessoal é descartada.
No caso de ser necessário remover um bilhete, então na lista de bilhetes guardados no cartão é seleccionado o item desejado para se eliminar e de seguida é requerido o PIN de autenticação e é actualizado o bloco de notas do cartão de cidadão.

Figura 7.12: Menu Cartão de Cidadão.

É importante realçar que o processo de comunicação entre o cartão de cidadão do utilizador e o website baseia-se no *middleware* desenvolvido, referido no capítulo anterior, auxiliado por um controlo *ActiveX* que permite que o utilizador interaja com o seu cartão no website através do protocolo *SSL*.

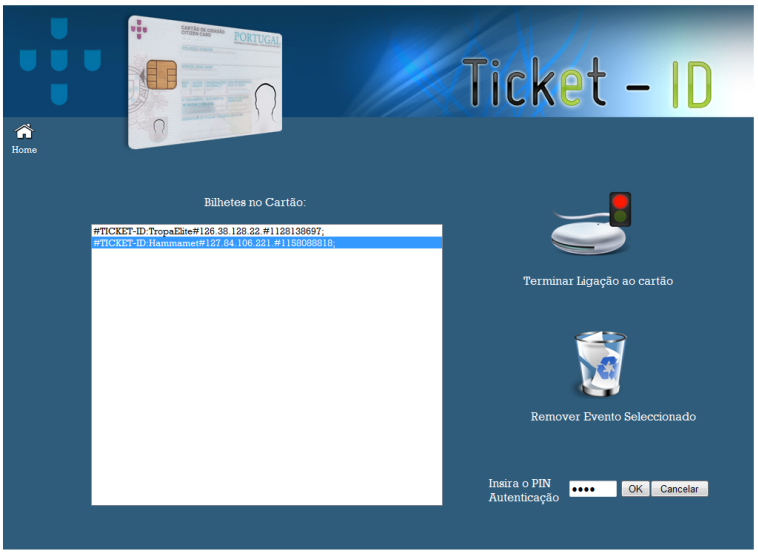

Figura 7.13: Menu Cartão de Cidadão.

7.2.2.7 Menu - Suporte

Tendo em conta que o processo de reserva apenas é concluído no agente de pagamento, importa saber os locais onde se podem encontrar os agentes de pagamentos.
Assim, neste menu apresenta-se um mapa ilustrativo de Portugal onde é possível consultar todos os agentes autorizados.

Figura 7.14: Menu Suporte.

7.2.2.8 Menu - Registar

Por último, o menu registar permite que novos utilizadores se associem ao sistema.

Figura 7.15: Menu Registar.

7.2.3 Módulo do Agente de Pagamentos

No módulo do agente de pagamentos podem realizar-se três operações distintas, isto é, a venda de bilhetes directa para qualquer evento, a conclusão de uma reserva via NFC, e a conclusão de uma reserva manualmente (observação visual da SMS de reserva).

Apresentam-se de seguida algumas ilustrações das funcionalidades do software desenvolvido na plataforma *.Net* mais precisamente em *WPF-Windows Presentation Foundation* a qual suporta as operações descritas.

Figura 7.16: Menu de Principal - Agente de Pagamento.

7.2.3.1 Agente de Pagamento - Menu de Venda Directa

O menu de venda directa consiste em vender bilhetes para eventos, sem que tenha sido feita uma reserva anteriormente, contudo o número de bilhetes disponíveis está limitado devido ao número de reservas realizadas através do website.

Neste menu o agente pode pesquisar o evento pretendido através do calendário ou via texto. Após seleccionado o evento pretendido são apresentados diversos detalhes do evento dos quais se destaca o número de bilhetes que ainda estão disponíveis. Seguidamente para processar o bilhete para o evento terá que inserir o contacto telefónico do cliente para o qual enviará o bilhete.

Tal como mostra a figura 7.17, o agente de pagamento do sistema *Ticket-ID* tem acesso a todos os eventos registados no sistema, isto deve-se à gestão dinâmica e eficaz dos conteúdos que foi implementada no sistema.

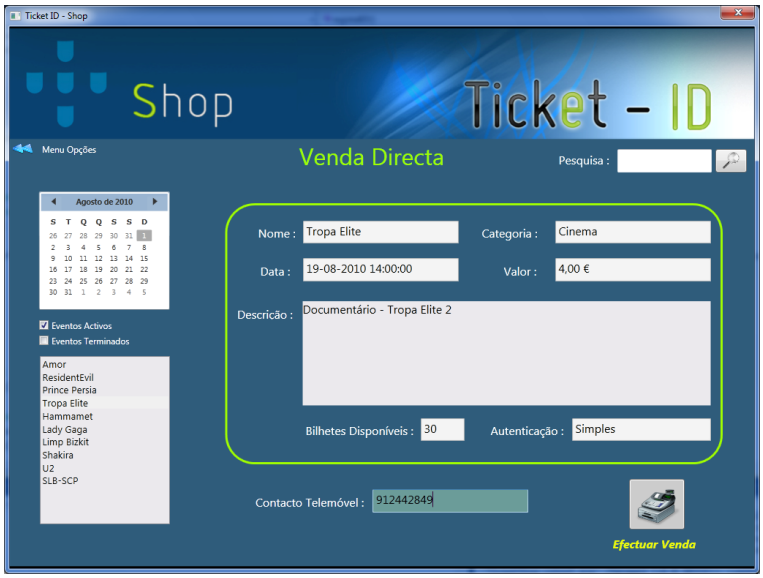

Figura 7.17: Menu de Venda Directa.

Seleccionado o evento para o qual se pretende adquirir um bilhete é agora necessário inserir o cartão de cidadão num terminal de leitura do agente e inserir o respectivo código PIN da assinatura para construir o bilhete electrónico associando as credenciais do cidadão (figura 7.18.

Figura 7.18: Emissão do bilhete com as credenciais do cartão de cidadão.

Terminada a construção e personalização do bilhete o agente de pagamento terá de o enviar ao cidadão, sendo que o sistema possibilita o envio do bilhete no formato de código de barras 2D via MMS para o contacto telefónico do cliente ou simplesmente via NFC para o telemóvel do cliente.

Figura 7.19: Opções de envio do bilhete (MMS/NFC).

Finalmente, recebido o código de barras 2D(*Qr-Code*) este está pronto a ser validado no comerciante (figura 7.20).

Figura 7.20: Ilustração do bilhete *QR-Code* recebido no telemóvel.

7.2.3.2 Agente de Pagamento - Menu de recepção de reservas (NFC)

No caso do cliente possuir uma reserva no seu telemóvel, o agente de pagamento pode receber os dados relativos à reserva interagindo com o telemóvel via NFC.
A imagem 7.21 demonstra uma interacção via NFC com o telemóvel do cliente (opcionalmente pode também ser usado um *smart card contactless*).

Figura 7.21: Menu de recepção de reservas - NFC.

Concluída a recepção dos dados relativos à reserva e confirmados pelo cliente, seguidamente o agente pode emitir o bilhete sendo este processo realizado da mesma forma como foi referido na imagem 7.19.

7.2.3.3 Agente de Pagamento - Menu de recepção de reservas (Manual)

O menu de recepção de reservas manuais (observação visual), foi desenvolvido tendo em conta que nenhum sistema deve ficar refém de qualquer tecnologia e como tal a alternativa mais simples e viável é a observação dos dados.
Assim na figura 7.22 pode observar-se que o agente de pagamento terá que inserir os dados chave relativos à reserva de forma manual.

Figura 7.22: Menu de recepção de reservas - Manual.

Por fim, caso os dados sejam validados pelo sistema, então o agente pode emitir o bilhete (figura 7.19) para o evento em causa.

7.2.4 Módulo do Comerciante

O módulo do comerciante também foi desenvolvido em *WPF*, com o intuito de oferecer ao comerciante um software simples e dinâmico. Apresentam-se de seguida algumas ilustrações do software desenvolvido e de todas as operações realizáveis.

7.2.4.1 Menu Principal - Comerciante

No terminal do comerciante, é apresentado um menu no qual é possível ao comerciante seleccionar o modo de validação dos bilhetes.
Tal como mostra a figura 7.23, o comerciante dispõe de várias opções tecnológicas para validar um bilhete, oferecendo deste modo ao sistema uma maior versatilidade, evitando limitações de utilização do sistema em caso de ocorrerem problemas técnicos com os equipamentos e também permite ao comerciante optar por soluções tecnológicas que achar mais conveniente. Por outro lado, como o processo de validação pode ser dinâmico (simples, forte, extra forte) isto implica que o sistema suporte qualquer um destes tipos de validação.

Figura 7.23: Menu Principal - Selecção da tecnologia de validação.

Seguidamente descrevem-se as quatro possibilidades de validação que possibilitam a leitura de um bilhete.

7.2.4.2 Menu de Leitura - Leitor *QR-Code*

No que diz respeito, à leitura de um bilhete no formato de código de barras 2D (*QR-Code*), o programa fica num modo de leitura em que aguarda que o leitor detecte um código de barras com um bilhete (*Ticket-ID*).

Figura 7.24: Leitor - Validação de um *QR-Code*.

Deste modo quando o leitor detecta um código de barras é descodificado o *Qr-Code* obtendo-se de seguida o talão de controlo (bilhete). Seguidamente é enviado o mesmo

à Base de dados para o validar. Caso o talão seja válido é confirmado ainda o tipo de validação do evento e dependendo deste tipo o processo de validação termina ou então muda para a validação forte/extra forte requerida para a validação do bilhete.

Importa referir que no caso da validação ser simples, o processo termina e é apresentada a informação relativa ao bilhete, tal como é possível de visualizar na imagem 7.24. O software têm ainda em comum às quatro possibilidades de validação animações que representa a leitura de um bilhete, o seu objectivo é dar um feedback dinâmico ao comerciante no acto da leitura. As animações dinâmicas, consistem em passados cinco segundos após a leitura e validação de um bilhete, limpar automaticamente toda a informação relativa a esse bilhete e iniciar novamente a leitura de um novo bilhete.

7.2.4.3 Menu de Leitura - *Webcam* (*QR-Code*)

Uma outra alternativa ao leitor *QR-Code* é a utilização de uma *Webcam* capaz de detectar em tempo real o padrão do código de barras. Detectado o padrão, o código de barras é descodificado e enviado para validação à Base de dados e caso seja válido é apresentada a respectiva informação tal como demonstrado na figura 7.25.

Figura 7.25: *Webcam* - validação de um (*QR-Code*).

7.2.4.4 Menu de Leitura - Leitor NFC

No que diz respeito ao modo de leitura via NFC, o comerciante ao seleccionar esta opção, o leitor NFC fica no modo activo, à espera de uma nova conexão. Quando o leitor interage com um dispositivo *contactless* (telemóvel, cartão *contactless*, *tag contactless*) este tenta identificar o respectivo bilhete emitido pelo sistema *Ticket-ID* e ao descodificar o talão de controlo que representa o bilhete, este é enviado à Base de dados para a sua validação, como mostra a imagem 7.26 e 7.27.

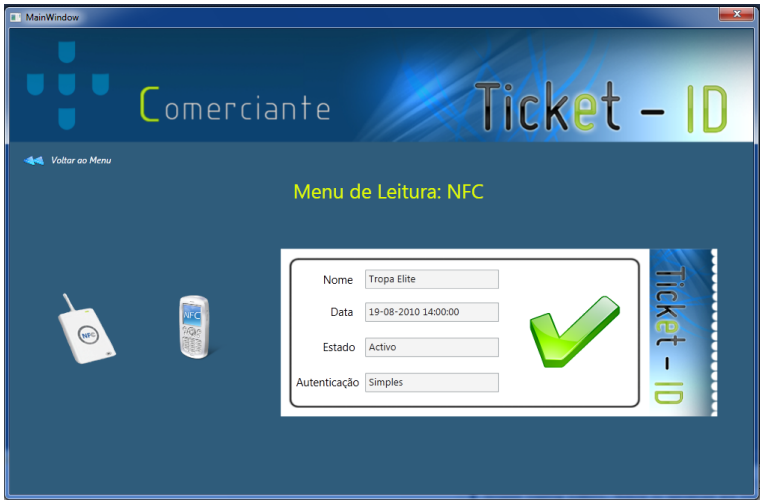

Figura 7.26: NFC - Bilhete validado com sucesso.

Figura 7.27: NFC - erro de validação.

7.2.4.5 Menu de Validação - Forte

O menu de validação forte, consiste em obter a pequena parte do eTicket que está armazenada no cartão do cidadão do cliente que representa um detalhe do bilhete, com o intuito de a juntar ao *eTicket* do comerciante. Unidos os *eTickets* o cliente assina os mesmos e obtém-se novamente o talão de controlo gerado que será validado na Base de dados.

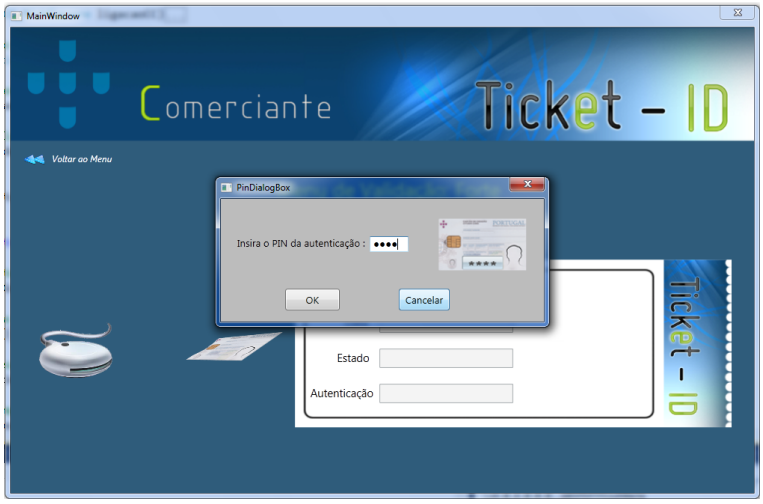

Figura 7.28: Menu de validação forte - Inserção do Pin da assinatura.

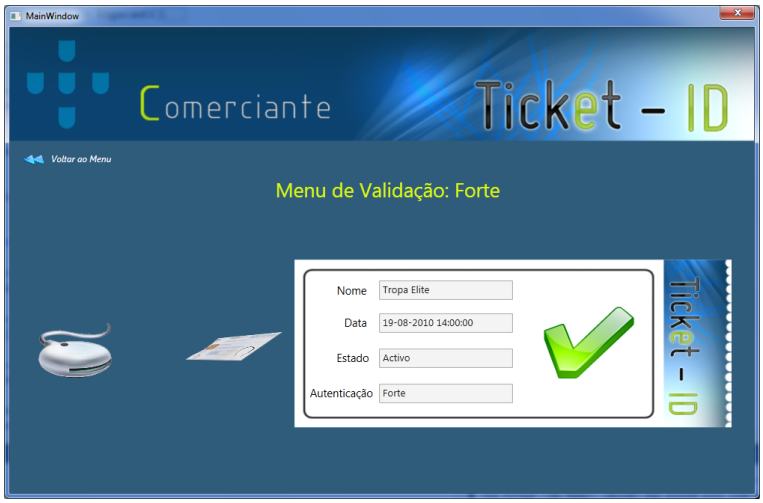

Figura 7.29: Menu de validação forte - representação de um bilhete válido.

No caso do modo de validação ser extra forte, então além de ser validado o bilhete e reconstruído o mesmo com as credenciais do cartão de cidadão é ainda necessário validar a identidade do cliente através da validação da impressão digital.

7.2.4.6 Menu de Validação extra forte

Por último, o menu de validação extra forte consiste sobretudo em validar a identidade do portador do cartão como foi referido, isto é, em termos de segurança o bilhete é validado no processo de validação forte e como tal este menu não acrescenta nada em termos de segurança sobre a concepção do bilhete, apenas em termos de identificação do portador do mesmo.

Figura 7.30: Menu de validação extra forte.

7.3 Diagramas de casos de uso

O objectivo de um diagrama de casos de uso de um sistema é mostrar a função deste sistema, isto é, quais são os possíveis usos do sistema, ignorando a forma como o sistema está organizado internamente. Mais precisamente, permite capturar o comportamento (funcionalidades) do sistema do modo como é visto pelos utilizadores.

Deste modo, utilizou-se a linguagem *UML-Unified Modeling Language* visto ser a linguagem mais comum e que se encontra normalizada para documentar, visualizar, especificar os artefactos de um sistema de software. A facilidade da notação permite que a comunicação entre as diversas entidades envolvidas no desenvolvimento de um produto de software seja simples e intuitiva.

7.3.1 Diagrama da plataforma de venda

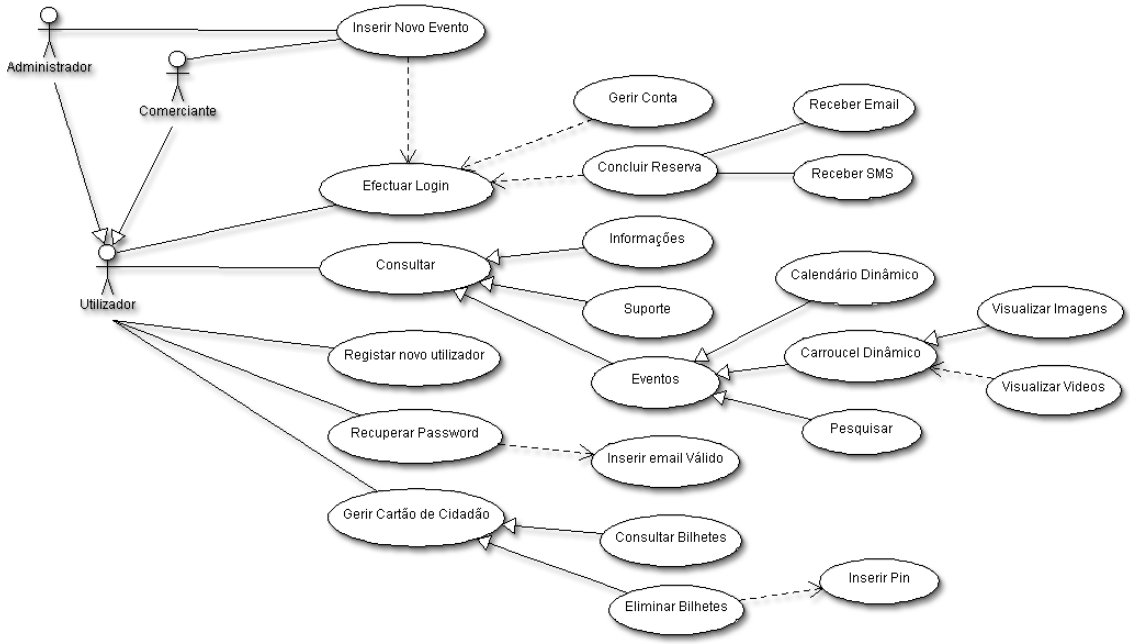

Figura 7.31: Diagrama de caso de uso da plataforma de venda - *Website*.

7.3.2 Diagrama do agente de pagamento

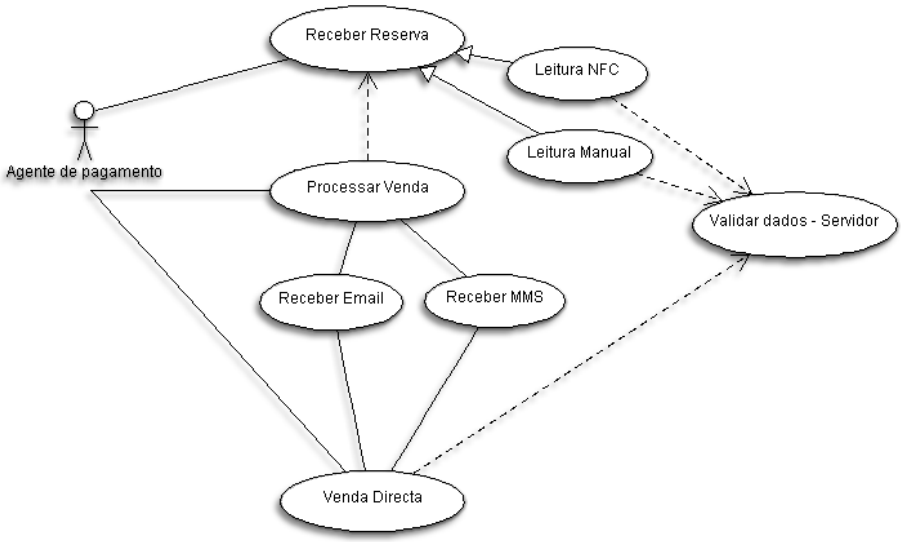

Figura 7.32: Diagrama de caso de uso do agente de pagamento - *Website*.

7.3.3 Diagrama do comerciante

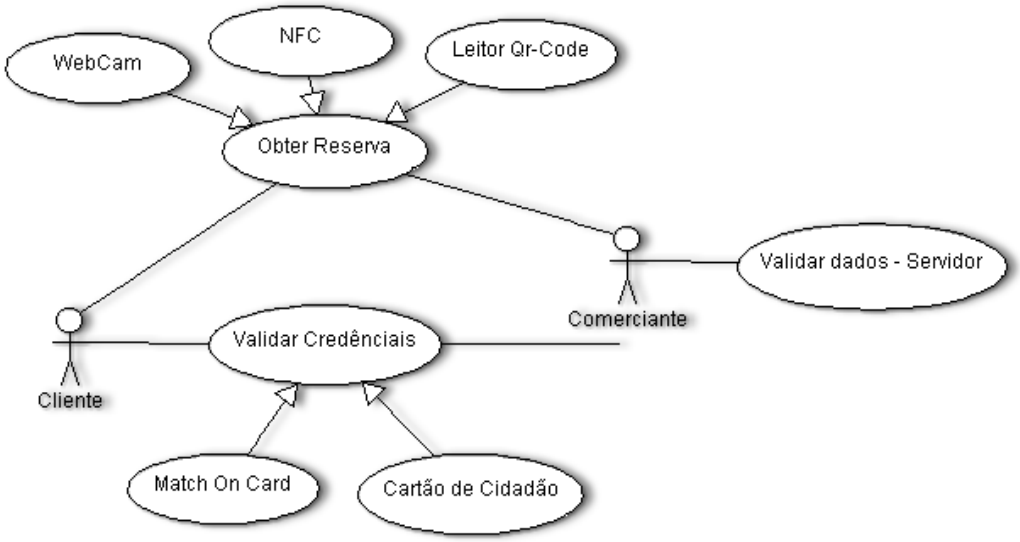

Figura 7.33: Diagrama de caso de uso do comerciante - *Website*.

7.4 Ferramentas utilizadas

Nesta secção descrevem-se as ferramentas utilizadas em termos de software e hardware no desenvolvimento de todo o sistema.

Software Utilizado:

Microsoft Visual Studio 2010	Microsoft Expression Blend 4
Microsoft Expression Design 4	Photoshop CS5
Microsoft Sql Server 2008	Precise Biometrics Toolkit
Middleware do CC Português	Acs - Acr122 SDK
QR-Code Encode/Decode SDK	Gliffy - Online Diagram Software
Microsoft Internet Information Services 7.0	ActiveXperts SMS/MMS Toolkit
Free Smtp Server 2.5	ArgoUML

Tabela 7.1: Lista de programas utilizados no desenvolvimento do sistema.

Hardware Utilizado:

Precise Biometrics 250 MC	ACS - Contactless reader (ACR122U-A2NR)
Leitor do cartão de cidadão	Webcam Creative NX Pro
Vodafone Mobile Connect K3565-Z	Sony Ericsson W910
Datalogic Magellan 1100i	Mifare 1Kbyte

Tabela 7.2: Lista de hardware utilizado.

7.5 Conclusões

O presente capítulo expõe de forma clara e objectiva o sistema desenvolvido em cada uma das suas fases, nomeadamente, a plataforma web de reserva de bilhetes, o software do agente de pagamento e do comerciante.

No entanto, é de realçar a multidisciplinaridade necessária ao desenvolvimento do sistema, nomeadamente a nível das diferentes tecnologias usadas e em termos de desenvolvimento dos módulos de software inovadores e dinâmicos que permitem uma interacção simples e segura.

Dito isto, importa salientar elementos como a Base de Dados implementada, que faz toda a gestão de eventos, reservas e vendas de forma dinâmica e automática o que permite que o sistema se adapte de acordo com as circunstâncias, sem que para isso seja necessário um trabalho de manutenção (*Back-Office*) muito trabalhoso e dispendioso.
Além da Base de Dados, também o modem GSM implementado no sistema é bastante inovador uma vez que permite o envio de reservas e bilhetes para o cliente rapidamente sem que isso implique necessariamente um custo acrescido para o cliente.
Por último, a inovação e utilização do cartão de cidadão no sistema permitiu identificar uma necessidade básica no funcionamento do sistema, a qual potenciou o desenvolvimento de um elemento inovador, isto é, a gestão da área reservada do cartão de cidadão através da plataforma Web.

É de realçar que o desenvolvimento de cada um dos módulos teve em consideração a realidade e os hábitos dos cidadãos, o que se reflectirá numa mais valia do ponto de vista da aceitação e implementação do sistema na sociedade.

Importa referir o uso de três tecnologias inovadoras na área da bilhética e que se tornaram uma mais valia para o correcto funcionamento do sistema.
Assim, os códigos de barras 2D - *QR-Code* auferem uma simplicidade maior na leitura electrónica de bilhetes através da leitura quer em papel ou no visor do telemóvel. Exemplo do sucesso da utilização desta tecnologia acontece nos eventos desportivos do *Sport Lisboa e Benfica*.

No caso da utilização da tecnologia NFC, esta é sem dúvida a mais recente inovação na área da bilhética, sendo que a evolução dos sistemas RFID possibilita a troca de mais informações e em tempo real entre dispositivos e neste caso o sistema *Ticket-ID* pretende também acompanhar a evolução tecnológica futura, onde os telemóveis vão interagir com diversos dispositivos. Um exemplo claro dos benefícios deste sistema é o uso do telemóvel como portador de bilhetes para os transportes públicos, onde os telemóveis não necessitam obrigatoriamente de ter bateria para concluir uma transacção.

Por fim, refere-se a relevância da tecnologia dos *smart cards*, neste caso o cartão de cidadão português, tem um papel fundamental em termos de segurança e inovação do sistema. A sua utilização permite que o cidadão português passe a ter um papel mais activo na utilização e domínio das potencialidades que o cartão de cidadão lhe pode proporcionar (rapidez, comodidade, segurança).

No próximo capítulo, tem como objectivo realizar uma análise comparativa do sistema *Ticket-ID* e outros semelhantes de forma a identificar os pontos fortes e críticos do sistema.

Capítulo 8

Análise do sistema *Ticket-ID*

O presente capítulo tem como objectivo fazer uma análise comparativa e uma consequente avaliação do sistema *Ticket-ID* com outros semelhantes.

8.1 Descrição sobre o caso de estudo da *Movensis*

Tal como foi descrito no capítulo 3, mais precisamente na secção 3.3.4, realiza-se agora uma análise mais detalhada sobre o caso de estudo da *Movensis*/CGD para pagamentos via telemóvel. Esta análise tem como objectivo servir de base comparativa ao sistema *Ticket-ID*. A escolha deste caso de estudo deve-se ao facto de ser um exemplo do novo sistema de pagamentos e evidencia ainda as dificuldades que um cidadão pode ter em se adaptar a este tipo de soluções.

Assim, o projecto apresentado pela empresa *Movensis* é bastante inovador do ponto de vista dos sistemas de pagamento. Contudo, existem factores neste conceito que em comparação com o sistema *Ticket-ID* revelam-se limitadores.

A solução da *Movensis* é neste momento uma simples utilização do telemóvel para transferir dinheiro da conta pessoal do cliente (promotora da projecto Caixa Geral de Depósitos) para a empresa que explora a máquina de vending (comerciante) , a fim de obter um produto.

O cliente tem em primeiro lugar de aceder à aplicação no telemóvel através de um

PIN e depois tem de identificar o número de série da máquina e enviar uma SMS com esta identificação mais o montante que pretende gastar. Este processo autoriza o banco (CGD) a transferir o dinheiro da sua conta pessoal para o comerciante, no caso de uma maquina de vending aparece o crédito disponível na própria maquina.

Finalmente é ainda necessária uma conexão à Internet através do telemóvel para finalizar a transacção.

Relativamente aos custos do produto, a este devem ser acrescidos os montantes referentes às tecnologias usadas, nomeadamente, o custo do envio da SMS e da ligação à Internet.

No caso de estudo apresentado existem diversas limitações que tornam a utilização do sistema um pouco complexo e demorado, nomeadamente, o processo por parte do cliente de descobrir e introduzir sempre o número de série da máquina de vending, o que do ponto de vista do cliente pode causar desinteresse por ser um processo pouco habitual.

Embora o caso de estudo se apresente sem dar grande importância às operadoras de redes móveis, na realidade é através delas que se estabelece a comunicação entre todos os intervenientes.

Resumindo, o projecto da Movensis/CGD não se revela prático do ponto de vista do utilizador segundo o feedback dos leitores da revista "Exame-Informática" [34] uma vez que existem diversos problemas em relação à usabilidade do sistema e em termos de segurança, nomeadamente as vulnerabilidades em torno do telemóvel e a utilização de mais um PIN.

Por outro lado, a interacção do utilizador com o telemóvel tem vindo a ser crescente, o que demonstra a aceitação de novas tecnologias de comunicação no telemóvel. De qualquer modo torna-se necessário apurar as reais necessidades do utilizador e sobretudo garantir a segurança dos dados e do dinheiro que é transferido nas compras electrónicas, visto que é o que separa a fronteira entre o sucesso e o fracasso do sistema.

A análise realizada a este caso de estudo pretende sobretudo mostrar uma das soluções existentes de modo a valorizar as potencialidades do sistema *Ticket-ID*.

8.2 Análise ao sistema *Ticket-ID*

Actualmente é um facto que a sociedade não está habituada a utilizar o telemóvel para aceder à sua conta bancária, embora existam soluções como o *MB-Phone* [67] suportada pela SIBS que permite o acesso à rede multibanco e consequentemente a realização de operações sobre a conta bancária.
Dito isto, um sistema que utilize o telemóvel para efectuar pagamentos utilizando a conta bancária apenas terá sucesso se for minimamente transversal a todos os bancos e como isso não acontece, a única solução actual é esta solução da SIBS.

Tendo em conta este impasse projectou-se o sistema *Ticket-ID* de forma a solucionar este problema e não a fazer parte dele. Assim, evitou-se o envolvimento directo das instituições financeiras e optou-se por introduzir o papel de agente de pagamentos, o qual é o responsável por todas as operações monetárias. Um agente de pagamentos é em tudo igual a actual rede de pagamentos *Payshop* ou *CTT*, onde as pessoas pagam os seus serviços, como de facto já acontece actualmente.

Deste modo, o sistema *Ticket-ID* baseia-se no conceito do utilizador reservar bilhetes para eventos através de um website, usando um computador ou um telemóvel, recebe uma SMS com a referência de pagamento que terá que liquidar num destes agentes à semelhança dos pagamentos por referência multibanco. O sistema ainda permite a venda directa de produtos nos locais dos agentes de pagamento o que torna o sistema ainda mais flexível.

Estes *modus* de funcionamento são simples e de acordo com os hábitos da sociedade e do comércio electrónico. Introduzindo a noção do agente de pagamento, este permite solucionar o problema dos pagamentos realizados via telemóvel, que associam a compra à conta bancária pessoal do cidadão. Repare que o *Ticket-ID* não introduz um novo

método de pagamento, nem utiliza o conceito de carteira electrónica, enquanto a sistema *Movensis* pode ser visto de facto como uma carteira electrónica.

Obviamente que esta decisão também se baseia em outros factores, nomeadamente no hábito que a sociedade já possui ao se deslocar a um agente de pagamentos para adquirir bilhetes para espectáculos, carregar o saldo do telemóvel, entre outros. Deste modo do ponto de vista do sistema desenvolvido é uma mais valia, uma vez que aproveita os hábitos do quotidiano da sociedade para a enquadrar e familiarizar com o sistema.

Em relação ao uso do cartão de cidadão no sistema, este deve ser visto de duas formas, isto é, do ponto de vista da segurança do sistema e do ponto de vista da sua utilização no processo de pagamento no agente de pagamento e possivelmente no comerciante.
Assim, no que diz respeito à sua utilização no sistema, é necessário ter em conta que o documento é sem dúvida o maior elemento de segurança que um cidadão possuí e como tal o seu uso no sistema oferece uma maior credibilidade e solidez. Por sua vez, a necessidade da sua utilização no acto de pagamento pode à primeira vista parecer algo novo, mas de facto a sua utilização é comparável a um pagamento com um cartão multibanco normal, onde apenas é necessário colocar o cartão no terminal e o respectivo PIN. Obviamente que é um hábito comum para o cidadão a forma como utiliza o cartão num agente de pagamento, a única diferença é a utilização inovadora do cartão de cidadão. Importa ainda referir, que facultar a identidade a um agente de pagamento pode parecer incomum, mas essa situação já acontece nos CTT em situações em que é necessário apresentar a identificação pessoal.

Por fim, importa referir que o telemóvel no sistema é utilizado sobretudo como transportador do bilhete e não como agente de pagamento. Isto deve-se ao facto de neste tipo de casos a maioria dos pagamentos são de baixo custo, o que limitam os sistemas no que diz respeito à sua usabilidade como se referiu anteriormente. Todavia o sistema *Ticket-ID* pretende que sejam realizadas quaisquer tipo de valores de pagamento, isto porque, consoante o tipo de pagamento também existem diferentes tipos de validação associadas obviamente ao cartão de cidadão.

Veja-se por exemplo, que o conceito do sistema vai desde a venda de um simples bilhete para um evento desportivo, onde a validação pode ser simples, como por exemplo a compra de um bilhete de avião onde o tipo de validação do bilhete requer outro tipo de credenciais. Isto para dizer que o sistema é capaz de abranger todo o tipo de eventos e de diferentes valores, uma vez que toda a segurança de compra, emissão e validação assenta sobre as credenciais pessoais de cada um. Importa ainda referir que muitos bilhetes hoje em dia são emitidos em papel e como tal são possíveis de se perderem e de serem utilizados por outrem, enquanto que no conceito do *Ticket-ID* o bilhete é electrónico e nem mesmo em caso de roubo do telemóvel ou do cartão de cidadão o bilhete se poderá perder.

Em suma, a utilização de simples códigos de barras e da utilização da tecnologia NFC também foi descartada pois em termos de segurança existem factores futuros e alheios ao sistema que podem vir a ser quebrados, tal como foi discutido na secção 2.3.3.4 e como tal, seria um prejuízo enorme do ponto de vista do negócio e do conceito em termos de confiança para a sociedade. Contudo, estas tecnologias revelam imensos potenciais e são utilizadas no sistema, mas apenas como transportadores dos bilhetes e não em termos de segurança pois isso diz respeito exclusivamente ao cartão de cidadão. Todavia caso sejam detectados no futuro problemas relacionados com cartão de cidadão e a tecnologia *smart card*, esta questão não é apenas problemática para o sistema *Ticket-ID*, mas sim para todo sistema de identificação Nacional e como tal existirão muitas entidades competentes interessadas em solucionar estes tipo de questões.

8.2.1 Análise sobre a implementação do sistema *Ticket-ID*

A maior dificuldade da implementação do sistema baseia-se no facto do preço acrescido que uma SMS/MMS recebida poderá ter no preço final do evento para o cliente. Note que contrariamente ao sistema Movensis onde o custo e o envio da SMS/MMS é directamente da responsabilidade do cliente, por sua vez no sistema *Ticket-ID* a SMS/MMS é enviada para o cliente e neste caso o custo é dos agentes de pagamentos/comerciantes.

Uma das soluções encontradas baseia-se na publicidade e nos parceiros envolvidos neste sistema, ou seja, qualquer MNO que se associe ao sistema pode beneficiar com a adesão de novos clientes devido às potencialidades inovadoras do sistema. Um exemplo, que hoje em dia acontece é a criação de um tarifário especial para este tipo de clientes, por um lado as operadores obtêm uma fonte de lucro e de participação neste sistema, por outro lado os clientes usufruem de um sistema de comunicações onde a troca de mensagens é gratuita.

O próximo e último capítulo apresenta conclusões finais sobre a presente dissertação e revela ainda futuros desenvolvimentos no sistema *Ticket-ID*.

Capítulo 9

Conclusão e trabalho futuro

O sistema *Ticket-ID* surge tendo em conta a evolução tecnológica na área dos pagamentos electrónicos usando o telemóvel. Actualmente estes já começam a ser utilizados para a compra e validação de bilhetes de espectáculos, pagamentos de serviços em substituição dos cartões bancários, cartões de fidelização e outros. A rápida evolução dos dispositivos móveis permite auferir novas características aos telemóveis que antes não existiam, resultando por isso na sua emergente aplicação em novas áreas como a bilhética. Dito isto, importa referir que na base do sistema *Ticket-ID* está um longo trabalho de investigação que permitiu associar os resultados produzidos a um projecto inovador que foi de acordo com as características e necessidades do mercado.

9.1 Conclusões

O início do processo de investigação, surgiu da pareceria com a *Multicert* e a sua participação no projecto *STORK*, referente ao uso de tecnologias RFID e NFC relacionadas com a identificação electrónica. A investigação levada a cabo no âmbito destas duas novas tecnologias permitiu o amadurecimento de conhecimentos e de novos conceitos em termos de funcionamento e de segurança.

Terminada esta investigação, surgiram rapidamente novas ideias relacionadas com a identificação electrónica, nomeadamente o uso do cartão de cidadão português com estas tecnologias. Nestes termos, decidiu-se fazer um *Brainstorming* sobre um

conjunto de temas em especifico que tivesse potencialidades de ver aplicados estes conceitos(e-ID e NFC/RFID). Foi juntamente com a *Multicert* e a *Commfides* que se idealizou o sistema *Ticket-ID*, tendo sido posteriormente a ideia amadurecida e definida exclusivamente pelo autor, a qual foi bem aceite por parte da *Multicert*.

Contudo a definição de qualquer sistema, é um processo complexa devido aos múltiplos actores do sistema (bancos, clientes, comerciantes, operadoras de redes móveis, agentes de pagamento), uma vez que existem conflitos de interesse entre eles e problemas associados em termos de delineamento dos papeis e objectivos dos vários actores nomeadamente no sistema de pagamento (capítulo 3). Apesar das dificuldades em se definir uma solução que fosse de concordância geral, foi encontrada uma bastante simples e semelhante aos métodos comuns de pagamento na sociedade.

Após a definição do tema e dos objectivos a alcançar, seguiu-se a metodologia de investigação a ser realizada para tornar possível atingir os objectivos definidos.

Assim, tendo em conta os objectivos do sistema *Ticket-ID* iniciou-se a investigação das potencialidades do cartão de cidadão e os seus processos de comunicação. Esta investigação foi a mais complexa e demorada, uma vez que devido à falta de documentação pública do Estado Português sobre o cartão foi necessário efectuar uma investigação incluindo o desenvolvimento duma metodologia para o processo da engenharia reversa que foi necessário para o desenvolvimento dum novo *middleware*. Esta investigação foi bastante proveitosa tendo resultado, além do próprio *middleware*, na publicação de dois artigos científicos. Foi ainda possível, graças a esta investigação, utilizar novas funcionalidades do cartão de cidadão (Assinatura Digital e Identificação Biométrica), as quais não estão disponíveis ao público em geral por parte do governo e que foram utilizadas de forma inovadora no sistema.

Paralelamente, foi ainda investigada a tecnologia de código de barras 2D *QR-code*, a qual se deve a dois factores importantes. Em primeiro lugar, decidiu-se que o sistema não deve ficar apenas refém de uma única tecnologia (NFC) devido aos inúmeros problemas associados a nível de usabilidade e de segurança. Por outro lado, a tecnologia do *QR-Code* já está actualmente implementada no mercado e com sucesso[16] junto do público em geral, ao invés o NFC que ainda não é integrada nos

telemóveis à venda em Portugal e como tal é desconhecida a sua adesão por parte da sociedade.

Por fim, terminada a investigação destas tecnologias foi possível projectar e desenvolver um sistema inovador, o *Ticket-ID*. Este resultou de facto num novo sistema, incluindo a definição da sua arquitectura, novos mecanismos de segurança e implementação dum protótipo totalmente funcional que englobou todas as funcionalidades idealizadas.

9.2 Trabalho futuro

Em termos de desenvolvimentos futuros do projecto estes podem dividir-se em aspectos de implementação e novos serviços.

9.2.1 Aspectos de Implementação

No que diz respeito a aspectos de implementação o sistema apresenta ainda duas limitações que podem ser facilmente solucionadas. Uma delas é o actual modelo de comunicação que envia SMS e MMS, o qual necessita de uma licença. Todavia pode ser desenvolvido este *toolkit* evitando por isso a aquisição de uma licença para o efeito.Igualmente em relação à validação biométrica, é necessária uma licença de forma a ser possível criar o *template* da impressão digital recolhida. Contudo, após uma breve investigação julga-se ser possível criar este *template* evitando por isso recorrer a *toolkits* de terceiros para construir apenas um simples *template* da impressão digital.

9.2.2 Novos serviços

Um serviço que o sistema *Ticket-ID* poderia acoplar seria o pagamento dos bilhetes através do telemóvel, contudo julga-se que a solução mais simples baseia-se na interacção com a plataforma *MBNet*, uma vez que já é utilizada em Portugal e bem compreendida pela sociedade.

Ainda assim é necessário investigar uma solução facilmente compreendida e segura, capaz de associar as credenciais do cartão de cidadão ao bilhete. Alguns exemplos interessantes podem ser vistos em [4] [46].

A projecção do sistema também pode ser alargada a outros países com *e-ID* e consequentemente a novos parceiros graças ao projecto STORK.

Tendo em conta que o cartão *e-ID* em outros países já possui um chip *contactless*, seria interessante investigar as potencialidades do mesmo de forma a torna o sistema ainda mais inovador e de simples utilização por parte dos cidadãos.

O desenvolvimento dum projecto-piloto, em particular na área dos transportes públicos, seria um próximo passo importante par testar aceitação e na facilidade de uso do sistema. Neste caso seria possível comprar os respectivos bilhetes usando o telemóvel nas máquinas automáticas de vending e associar aos mesmos as respectivas credenciais do cartão de cidadão do cliente, associando deste modo a identidade pessoal ao bilhete electrónico.

Por fim, seria interessante divulgar este trabalho na comunicação social e na comunidade académica, esforço que já começou com a participação na segunda conferência *"eID & ePassport Conference"*, em Outubro de 2010 em Atenas.

Referências

[1] ISO 7816. *SmartCard Standard ISO7816*, 2009. http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx.

[2] ACS. *Application Programming Interface*, 2008. http://www.acs.com.hk/.

[3] AMA. *Site Cartão de Cidadão Português*, 2010. http://www.cartaodecidadao.pt.

[4] ARCADA. *The Mobile Finnish Identity Certificate*, 2007. http://people.arcada.fi/~goran/advsecu/mobile_fineid.pdf.

[5] Batina, Guajardo, Kerins, Mentens, Tuyls, and Verbauwhede. Public-key cryptography for rfid tags. 2008.

[6] Precise Biometrics. *Precise Biometrics - 250MC*, 2010. http://www.precisebiometrics.com/?id=2718&cid=2723.

[7] Bird, Conrado, Guajardo, Maubach, Scrijen, Skoric, Tombeur, Thueringer, and Tuyls. Algsics - combining physics and cryptography to enhance security and privacy in rfid systems. 2007.

[8] Edmundo Monteiro Fernando Boavida. *Engenharia de Redes Informáticas*. FCA, 2007.

[9] Wen-Yuan Chen and Jing-Wein Wang. Nested image steganography scheme using qr-barcode technique. 2009.

[10] Zhiqun Chen. *Java Card Technology for Smart Cards*. Sun, 2000.

[11] European Comission. *RFID the Internet of Things*, 2009. http://www.iot-visitthefuture.eu.

[12] V-ONE Corporation. *PC/SC Specification Information Paper*, 1998. http://www.firstnetsecurity.com/library/v1/PC-SCInfoPaper-95.PDF.

[13] Damme and Wouters. Pratical experiences with nfc security on mobile phones. 2005.

[14] Deursen and Radomirovic. Security of rfid protocols - a case study. 2007.

[15] Giesecke & Devrient. *NFC Project - Touch & Travel*, 2009. http://www.gi-de.com/portal/page?_pageid=44,137589&_dad=portal&_schema=PORTAL.

[16] Sport Lisboa e Benfica. *Bilheteira Online - Códigos de Barra 2D*, 2010. http://www.slbenfica.pt/Ajuda/ajuda_bilhetesporsms.asp.

[17] Enisa. *Security Issues in the Context of authentication using mobile devices*, 2008. http://www.enisa.europa.eu.

[18] Enisa. *Privacy and Security Risks when Authenticating on the Internet with European eID Cards*, 2009. http://www.enisa.europa.eu.

[19] Enisa. *Privacy Features of European eID Card Specifications*, 2009. http://www.enisa.europa.eu - Fevereiro de 2009.

[20] Visa Europe. *The wave and pay alternative to cash for low value transactions*, 2008. http://www2.visaeurope.com/pressandmedia/factsheets/visacontactless.jsp.

[21] Klaus Finkenzeller. *RFID-Handbook, 2nd edition*. Wiley, 2003.

[22] Gemalto. *Operating Software in Secure Electronic Documents*, 2008. http://www.gemalto.com.

[23] Gemalto. *A complete operated service for managing the Near Field Communications application lifecycle*, 2010. http://www.gemalto.com/brochures/download/allynis_mobile_nfc.pdf.

[24] Gemalto. *Gemalto Integrates DESFire Transport Card into NFC Mobile Phone*, 2010. http://www.smartcardalliance.org/articles/2010/02/15/.

[25] Gemalto. *Maximizing opportunities in the mobile NFC marketplace*, 2010. http://www.gemalto.com/brochures/download/nfc_mobile_operators.pdf.

[26] Gemalto. *Nice - mobile contactless city*, 2010. http://www.nfcnews.com/2010/05/21/gemalto-announces-a-pair-of-european-nfc-partnerships.

[27] Estonian Government. *Estonian eID card - citizens can use it to buy e-tickets for public transport*, 2009.

[28] Estonian Government. *Estonian eID card - e-tickets for public transport*, 2009. https://www.pilet.ee/cgi-bin/splususer/splususer.cgi?lang=en http://www.id.ee/.

[29] Porvoo Group. *Piloting e-ID Interoperability*, 2009. http://porvoo15.a-sit.at/pdf_etc/presentations/Roessler_P15_stork.pdf.

[30] GSMA. *Mobile NFC technical guidelines*, 2007. http://www.gsmworld.com/documents/gsma_nfc2_wp.pdf.

[31] GSMA. *Pay-Buy-Mobile - Business Opportunity*, 2007. http://www.gsmworld.com/documents/gsma_nfc_tech_guide_vs1.pdf.

[32] GSMA. *Pay-Buy-Mobile Business Opportunity - Public White Paper Analysis*, 2007. http://www.gsmworld.com/documents/.

[33] Nick Hughes and Susie Lonie. M-pesa: Mobile money for the unbanked. 2009.

[34] Exame Informática. *Movensis e CGD vão estrear pagamentos por telemóveis*, 2010. http://aeiou.exameinformatica.pt/movensis-e-cgd-vao-estrear-pagamentos-por-telemovel-video=f1007055.

[35] European Telecommunications Standards Institute. *SWP - Single Wire Protocol*, 2010. http://pda.etsi.org/pda/queryform.asp.

[36] ISO7816. *APDUs*, 1999-2009. http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4.aspx.

[37] Ari Juels, Ronald L Rivest, and Michael Szydlo. The blocker tag: Selective blocking of rfid tags for consumer privacy. 2003.

[38] Kadambi, Li, and Karp. Nfc - based secure mobile payment. 2009.

[39] Kan, Teng, and Chou. Applying qr code in augmented reality applications. 2009.

[40] Rajan Kumar and Gurman Dhillon. Rfid-an emerging aidc technique. 2008.

[41] Peeter Laud and Meelis Roos. Formal analysis of the estonian mobile-id protocol. 2008.

[42] Yan Liang and Chumming Rong. Rfid system security using identity-based cryptography. 2008.

[43] Tarvi Martens. *Estonia - the country with identification infrastructure*, 2006. `https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ThirdWorkshopPresentations/2006-02-09_modinis-idm-ws3_presentation_martens.pdf`.

[44] mGovLab. *Global Acceptance of Mobile ID card*, 2004. `http://www.mgovlab.org`.

[45] Mizuno, Yamada, and Takahashi. Authentication using multiple communication channels. 2005.

[46] Axia A306 Mobile. *Mobile Phone Support e-ID and NFC*, 2010. `http://www.fifthmedia.biz/mobile.htm`.

[47] Vesna Hassler Martin Manninger Mikhail Gordeev Christoph Muller. *Java Card for E-Payment Applications*. Artechhouse, 2001.

[48] Collin Mulliner. Vulnerability analysis and attacks on nfc mobile phones. 2009.

[49] Oberthur. *Bank ID for SEB*, 2009. `http://www.Oberthur.com`.

[50] Roger C. Palmer. *The Bar Code Book: Fifth Edition - A Comprehensive Guide To Reading, Printing, Specifying, Evaluating, And Using Bar Code and Other Machine-Readable Symbols*. Trafford Publishing, 2007.

[51] Agência para a Modernização Administrativa. *Autenticação forte e assinatura digital qualificada*, 2010. http://www.cartaodecidadao.pt/index.php?option=com_content&task=view&id=38&Itemid=35&lang=pt.

[52] Agência para a Modernização Administrativa. *Autenticação forte e assinatura digital qualificada*, 2010. http://www.pofc.qren.pt/ResourcesUser/Avisos/20090618_5_AutenticacaonoCartaodeCidadao.pdf.

[53] Agência para a Modernização Administrativa. *Site do Cartão de Cidadão*, 2010. http://www.cartaodecidadao.pt/.

[54] Annika Paus. Nfc in cell phones. 2007.

[55] Pcausa. *USB Snoop Pro*, 2007. http://www.pcausa.com/Utilities/UsbSnoop/.

[56] Norbert Pohlmann, Helmut Reimer, and Wolfgang Schneider. *ISSE/SECURE - Securing Electronic Business Processes*. Springer Science, 2007.

[57] PORTIORESEARCH. *Mobile Payments*, 2008. http://www.portioresearch.com.

[58] Wolfgang Rankl. *Smart Card Applications - Design models for using and programming smart cards*. Wiley, 2007.

[59] Mikael Ricknas. *Estonia to Use Mobile Phones to Simpify E-voting*, 2008. http://www.pcworld.com/article/155490/estonia_to_use_mobile_phones%_to_simpify_evoting.html.

[60] Ludovic Rousseau. *Provided tools*, 2008. http://ludovic.rousseau.free.fr/softwares/pcsc-tools/smartcard_list.txt.

[61] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition*. Wiley, 1996.

[62] Christoph Seidler. Rfid - opportunities for mobile telecommunications services. 2005.

[63] Uwe Hansmann Martin Nicklous Thomas Schack Achim Schneider Frank Seliger. *Smart Card Application - Development Using Java*. Springer, 2002.

[64] Philips Semiconductors. *Data Sheet: MiFare Standard Card IC - MF1 IC S50*, 2001. http://www.synometrix.com/MF1_20S501_Data_Sheet.pdf.

[65] Alexander Shevelev. *Cheef's Personal Site*, 2010. http://cheef.ru/docs/HowTo/.

[66] SIBS. *SIBS MB-Phone*, 2010. http://www.sibs.pt/pt/mb/prodserv/mbphone/.

[67] SIBS. *Vodafone MB-Phone*, 2010. http://www.vodafone.pt/main/Particulares/Servicos/Multibanco_no_Telemovel/Telemultibanco.htm.

[68] Ian Sommerville. *Software Engineering (9th Edition)*. Addison Wesley, 2010.

[69] M.M.J. Stevens. On collisions for md5. Master's thesis, Eindhoven University of Technology, 2007.

[70] Swetake. *How to create QRcode*, 2007. http://www.swetake.com/qr/qr1_en.html.

[71] Innovision Research Technology. Nfc in the real world. 2008.

[72] Tedjini and Vuong. Rfid - a technology for the future. 2007.

[73] Blog Telemóveis. *Noticia Aplicações do QR-Code*, 2009. http://www.telemoveis.com/news/item.asp/t/Codigos-de-Barras-2D/id/22730.

[74] Frankfurt U-Bahn. *Transport Network gets NFC and QR-Code Smart-Posters*, 2010. http://www.nearfieldcommunicationsworld.com/2010/04/27/.

[75] UCMA/UMIC/DGRN. *Verificação por via da impressão digital*, 2007. http://www.pofc.qren.pt/ResourcesUser/Avisos/7_Guia%20Pr%C3%A1tico%20de%20utiliza%C3%A7%C3%A3o%20do%20Cart%C3%A3o%20de%20Cidad%C3%A3o%20.pdf.

[76] UNISYS. *Globally trusted standards for identification credentialing pratices and processes*, 2008. http://www.unisys.com.

[77] Ronald Leenes Bart Priem Carla van de Wiel Karolina Owczynik. *Towards pan-European recognition of electronic IDs*, 2009. https://www.eid-stork.eu/dmdocuments/public/D2.2_final._1.pdf.

[78] Simão Melo de Sousa Vasco Nicolau, Paul Crocker. Sniffing with the portuguese identify card for fun and profit - *9th European Conference on Information Warfare and Security*. 2010.

[79] Visa. *Visa mobile payments service for point-of-sale transactions using NFC technology*, 2009. http://corporate.visa.com/media-center/press-releases/press921.jsp.

[80] Vivotech. *NFC Mobile Payment Pilot to Date for Citi in India*, 2010. http://www.vivotech.com/newsroom/press_releases/ViVOtech_Wins_2_Major_Awards.asp.

[81] RENFE & Vodafone. *Spanish Train - Allows Mobile Ticketing*, 2009. http://www.bwcs.com/news_detail.cfm?item=10872.

[82] Wikipédia. *Middleware*, 2010. http://en.wikipedia.org/wiki/Middleware.

[83] André Zúquete. *Segurança em redes informáticas*. FCA, 2010.