ISEL
INSTITUTO SUPERIOR
DE ENGENHARIA DE LISBOA

Estudo e Desenvolvimento de Sistema de Cobrança de Portagens baseado em NFC

Tese para obter o grau de Mestre em

Engenharia Eletrónica e Telecomunicações

Autor:

Filipe Miguel Andrez Palhinha

Juri:

Orientador: Professor Doutor António João Nunes Serrador

Presidente de mesa: Professor Doutor Mário Pereira Véstias

Vogal: Professor Doutor João Carlos Amaro Ferreira

Dezembro 2014

Agradecimentos

Este projeto de mestrado não teria sido desenvolvido sem o incentivo e apoio de várias entidades e pessoas que me apoiaram e incentivaram no decorrer do mesmo, assim aqui ficam os meus sinceros agradecimentos.

Os merecidos vão para a instituição de ensino ISEL por permitir e investir em projetos como este que permitem a aquisição de novos conhecimentos tanto para a instituição como para mim. Ao Eng.º António Serrador pela iniciativa de proposta deste projeto e pela confiança em mim depositada para o estudar e desenvolver. Aos meus colegas pelos constantes conselhos e opiniões no decorrer do desenvolvimento do hardware e deste documento. E por fim à minha família pelo apoio e incentivo que me proporcionaram não só no decorrer deste projeto mas em todo o meu percurso académico que aqui me conduziu.

Resumo

Este projeto de mestrado visa estudar e desenvolver uma solução para cobrança e identificação em portagens, em que é necessário cobrar aos utilizadores as taxas associadas à utilização de vias concessionadas reservadas a veículos.

Com este projeto aborda-se e estuda-se a utilização da tecnologia de comunicação NFC existente nos *Smartphones* como meio de o utilizador se identificar numa portagem.

A tecnologia Near Field Communication (NFC) permite que os dispositivos comuniquem sem fios a uma distância muito próxima, sendo uma das mais importantes tendências nos telemóveis hoje em dia. Os pagamentos via telemóvel é uma das mais esperadas aplicações visto que cada pessoa transporta um hoje em dia. A tecnologia NFC é uma excelente promotora para o avanço destes pagamentos devido à sua segurança, facilidade de uso e versatilidade.

O uso desta tecnologia para fazer pagamentos é controlada por grandes empresas que mantêm o hardware que permite as transações seguras para pagamentos para uso próprio e longe do desenvolvimento para terceiros.

Este projeto procura estudar e desenvolver um sistema de pagamento de portagens, desenvolvendo um método para que os terminais se identifiquem unicamente, sem necessitar de uma ligação sem fios para se autenticarem.

Do lado do leitor é usado o sistema embebido *Raspberry Pi* com um *transceiver* NFC e uma antena, do outro lado um *Smatphone* com sistema operativo Android e uma aplicação para identificar e interagir com o utilizador.

Para implementar uma comunicação bidirecional através de NFC o leitor emula uma *tag* para efetuar a troca de dados e contornar a limitação do sistema operativo Android em manter um fluxo de dados contínuo nos dois sentidos.

Para efetuar a transação o utilizador apenas necessita de encostar o telemóvel ao leitor e esperar pelos dados de confirmação enviados pelo leitor da portagem.

Palavras chave: *Near Field Communication*, pagamentos, portagens, Android.

Abstract

This master's project aims to study and develop a solution for collection and identification in tolls, where it is necessary to charge users fees associated with use of concession lanes reserved for vehicles.

With this project up addresses the use of existing NFC communication technology in smartphones as a means for the user to identify in a toll.

The Near Field Communication (NFC) technology allows devices to communicate wirelessly within a very close distance, being the most important trends in mobile phones today. Payments via mobile phone is one of the most anticipated applications since each person carries one today. NFC is an excellent promoter for the advancement of these payments because of its safety, ease of use and versatility.

The use of this technology to make payments is controlled by large companies that keep the hardware that allows secure payments to itself and away from development for third parties transactions.

This project aims to study and develop a way to uniquely identify a handset using a local secure protocol developed to this purpose, without a wireless connection to authenticate securely.

On the side of the reader is used a Raspberry Pi embedded system with a NFC transceiver and an antenna, on the other side a mobile phone with Android operating system and an application developed to identify and interact with the user.

To implement two-way communication via NFC, the reader emulates a tag to exchange data and work around the limitation of the Android operating system to maintain a continuous flow of data in both directions.

To make the transaction the user only needs to holding the phone in the reader and wait for confirmation of data sent by the toll reader.

Keywords: Near Field Communication, payments, tolls, Android.

Indíce

Índice de figuras

Índice de tabelas

Lista dos principais acrónimos

BPSK	Binary phase-shift keying
CC	Capability Container
C-APDU	Command Application Protocol Data Unit
ID	Identificador
LLCP	Logical *Link* Control Protocol
NDEF	NFC Data Exchange Format
NFC	Near Field Communications
NFC-WI	NFC Wired
PCB	Printed circuit board
RF	Radio frequência
RFID	Radio-Frequency Identification
RFU	Reserved for future use
R-APDU	Response Application Protocol Data Unit
SCUT	Sem custos para os utilizadores
SWP	Single Wire Protocol
TVL	Bloco TVL do ficheiro CC

1. Introdução

As portagens hoje em dia são destinadas a cobrar ao utilizador uma taxa associada à utilização de vias concessionadas, podem aparecer na forma de barreira física que obriga a paragem ou abrandamento para efetuar a transação, ou na vertente de pórtico, que não implica paragem nem abrandamento. Nas barreiras físicas a cobrança é feita de variadas maneiras, como dinheiro, cartão de débito/crédito, que implicam a paragem da viatura, ou por identificação eletrónica, que no caso de estar implementado na barreira física apenas implica abrandamento. A vertente de pórtico que não implica abrandamento, aplicado em Portugal [1] em 2010 em algumas Autoestradas SCUT (Sem custos para os utilizadores),é também utilizado um dispositivo eletrónico de identificação associado ao veículo, tal como na barreira física, ou caso o veículo não possua este dispositivo a cobrança é feita através de um sistema de identificação de matrículas.

O aparecimento da tecnologia de comunicação *Near-field Communication* (NFC) nos *Smartphones* veio desencadear um alargar de funcionalidades destes dispositivos, oferecendo uma maneira de estes comunicarem apenas quando estão muito próximos de outro dispositivo NFC. Esta característica vem trazer uma grande evolução na segurança da comunicação, onde apenas dispositivos que estejam numa proximidade de 4cm [2] conseguem comunicar entre si, sendo muito difícil intercetar a comunicação fora deste alcance.

Este projeto de mestrado visa usar a comunicação NFC presente nos *Smartphones* dos utilizadores das vias concessionadas, que previamente foram registados no sistema da operadora da via, para os identificar e posteriormente cobrar as taxas relativas à sua utilização. O *Smartphone* passa a ser o identificador pessoal daquele utilizador à semelhança do identificador usado no sistema da Via Verde [3] em que o mesmo se coloca no vidro da viatura e comunica com a antena presente na barreira física para fazer a identificação.

1.1. Enquadramento

Este projeto de mestrado está inserido num ambiente de cobrança e identificação em portagens, em que é necessário cobrar aos utilizadores as taxas associadas à utilização de vias concessionadas reservadas a veículos.

Ao entrar ou sair de uma via concessionada, atualmente o utilizador dispõe de várias formas para efetuar o pagamento: dinheiro, identificador Via Verde, ou identificação por matrícula. Com este projeto aborda-se e estuda-se a utilização da tecnologia de comunicação NFC existente nos *Smartphones* como meio de o utilizador se identificar numa portagem.

1.2. Motivação

O desenvolvimento deste projeto de mestrado é motivante na medida em que as aplicações móveis hoje em dia são uma aposta de muitas empresas para fornecer serviços ao utilizador e para o mesmo poder gerir e centralizar a sua informação no *Smartphone*. Outro ponto motivante é o facto de trabalhar com o sistema operativo Android e com a tecnologia NFC ser uma novidade para mim, contribuindo assim para alargar o meu leque de conhecimento.
Outro dos pontos motivantes é o facto de ser o primeiro projeto de mestrado no ISEL a usar a tecnologia NFC de um *Smartphone* para comunicar com um leitor externo também programado para o efeito, deixando alguma experiência do uso desta tecnologia na instituição.

1.3. Objetivos

O objetivo deste projeto visa desenvolver os dois lados do sistema de cobrança de portagens, dum lado uma aplicação desenvolvida em Android que interaja com o utilizador e com os periféricos NFC existentes no Smartphone, do outro lado um leitor que detete a presença de um dispositivo NFC e efetue a troca de dados com o mesmo.
Com este projeto procura-se desenvolver um sistema de fácil manuseio por parte do utilizador, rápido e flexível, para que a transação seja efetuada com o mínimo de interação por parte do utilizador, oferecendo comodidade e conforto.

1.4. Estrutura do trabalho

Este trabalho começa no Capítulo 2, o Estado da arte, por fazer um apanhado do que é a tecnologia NFC, onde surgiu e como começou a ser usada. Em termos do hardware utilizado é apresentado que estrutura de antena e que tipo de radiação a tecnologia NFC usa para transferir energia, como é estruturado um *Smartphone* que contenha a tecnologia NFC e os diferentes modos de comunicação em que pode operar. Por fim faz-se uma análise de um

produto que permite fazer pagamentos através de NFC, aborda os problemas de segurança inerentes a este tipo de transação e que medidas de segurança são oferecidas pelo hardware e normas existentes.

No Capitulo 3, o Desenvolvimento, estuda-se o controlador NFC que vai ser usado do lado do leitor, tal como o restante hardware de processamento. Para uso do hardware avalia-se que tido de protocolo, normas e bibliotecas poderão ser usados para implementar uma comunicação NFC bidirecional para troca de dados entre a aplicação Android e o leitor da portagem. No fim do capítulo apresenta-se como está estruturado e como foi desenvolvido o software do lado do *Smartphone* e do lado da portagem.

O Capitulo 4 apresenta os resultados relativos à implementação que foi estudada e desenvolvida no Capitulo 3, tais como distância máxima de comunicação entre o *Smartphone* e o leitor da portagem, tempos de transação detalhados e falhas do sistema.

2. Estado da arte

2.1. Introdução à tecnologia NFC

Near Field Communication (NFC) é uma tecnologia de Radio Frequência (RF) para comunicações de curto alcance que troca dados entre dois dispositivos, como leitores, cartões, telemóveis, sensores, etc.

NFC é caracterizado como uma tecnologia de comunicação de muito curto alcance com muito potencial, particularmente quando é aplicada em *Smartphones*. A tecnologia permite que o *Smartphone* interaja com posters, revistas, e com produtos que ainda estejam na loja, tal interação pode dar início a uma pesquisa relacionada com o conteúdo naquele momento. Outra aplicação do NFC está relacionado com a carteira eletrónica para fazer pagamentos, usando o *Smartphone* da mesma maneira que se usaria o cartão de crédito. Mas o NFC é uma tecnologia recente, os dispositivos com NFC ainda estão a ser introduzidos no mercado, os desenvolvimentos e implementações com esta tecnologia começam a aparecer por todo o mundo.

NFC é uma especificação desenvolvida pelo NFC Forum [4], um consórcio global de hardware, aplicações e software, empresas de cartões de crédito, bancos, operadores de redes, e outros que estão interessados em desenvolver e especificar esta tecnologia promissora.

A tecnologia rádio NFC opera em curto alcance, a uma frequência de 13.56MHz, com transferência de dados até 424 kb/s. A comunicação NFC ocorre quando dois dispositivos compatíveis se aproximam a uma distância de cerca de 4cm. O facto do alcance da transmissão ser muito curto, as transações baseadas em NFC são inerentemente seguras.

A grande motivação do NFC em dispositivos móveis é a integração da informação pessoal e privada como um cartão de crédito ou um cartão de débito. No entanto, a segurança é um aspeto muito importante, vindo a ser uma inovação no NFC. Na tecnologia antecessora ao NFC, o RFID, mecanismos como blindagem seriam necessários para prevenir o acesso não autorizado à comunicação, pois mesmo os dispositivos passivos como as *tag*s RFID podem ser lidas até 10m.

Os sistemas de identificação digitais tiveram início no código de barras (leituras óticas), tal tecnologia disponibilizava uma codificação a uma dimensão variando a distância entre barras

e a sua espessura, o que se mostrou limitado pelo espaço ocupado e também pela facilidade na sua replicação e distribuição. Após os códigos de barras surgiu a tecnologia dos cartões com banda magnética, que continham a informação guardada em pequenas partículas magnéticas gravadas na fase de produção, os dados presentes na banda magnética poderiam também ser copiados por um leitor de bandas magnéticas e usados por terceiros. Após isso surgiu a tecnologia RFID em que a transferência de dados já era feita por meio de ondas rádio e a informação estava guardada num chip integrado permitindo um maior armazenamento de informação e segurança tornando a cópia e contrafação mais difícil. Com o aparecimento dos cartões inteligentes (*Smart Cards*), o nível de segurança foi significativamente aumentado, já contendo microprocessadores com vários níveis de segurança e chaves privadas internamente armazenadas para cifrar a informação.

A especificação detalhada do NFC pode ser encontrada na norma ISO 18092 [5]. É um seguimento da tecnologia da *RF Identification* (RFID). O aparecimento do RFID começou na Segunda Guerra Mundial, onde a força aérea Inglesa identificava os seus aviões. O primeiro aparecimento comercial da tecnologia foi em 1960 na forma de *tag*s RFID de 1 bit para segurança em lojas, que ainda é muito usado. Em 1990 o RFID começou a ser ainda mais comum e utilizado em controlo de acessos e cobrança de portagens [6]. Em 2002 a tecnologia NFC foi desenvolvida pela NXP e Sony.

Em grande parte, como o NFC é uma evolução do RFID e dos cartões inteligentes (*Smart Cards*), é compatível com a maioria dos sistemas RFID e sistemas sem fios dos *Smart Cards*, mas a sua arquitetura tem um princípio diferente. Enquanto os *Smart Cards* sem fios têm uma estrutura de leitor/*tag*, um dispositivo NFC pode ser ambos, leitor e emissor.

O formato de troca de dados NFC, NFC Data Exchange Format (NDEF), foi desenvolvido para permitir que as *tag*s RFID e os cartões sem fios fossem compatíveis com aplicações NFC. A característica chave do NFC é que a interface de comunicação sem fios tem uma distância limite de operação de cerca de 10cm.

Em 2004, foi fundado o "NFC Forum" pela Philips, Nokia e Sony. O objetivo do "NFC Forum" é permitir que os utilizadores tenham acesso ao conteúdo e serviços de uma maneira intuitiva, levando a um mundo de comércio seguro e de conectividade em que os utilizadores podem aceder e pagar por serviços físicos e digitais em qualquer lugar, a qualquer momento, usando qualquer dispositivo compatível com NFC. A sua missão é desenvolver a tecnologia

NFC criando normas que assegurem a interoperabilidade entre dispositivos e serviços, encorajando o desenvolvimento de produtos usando as especificações do "NFC Forum", educando globalmente o mercado com a tecnologia NFC, e também garantir que os produtos cumprem as normas definidas pelo "NFC Forum" [7].

Ao adicionar uma nova funcionalidade de um cartão sem fios NFC a um telemóvel, criou-se um telemóvel que é capaz de comunicar com outros dispositivos NFC quando está próximo destes. Esta combinação de telemóvel e tecnologia NFC permite aos utilizadores usar serviços inovadores, podendo aceder a inúmeros serviços NFC no dia-a-dia apenas com um telemóvel, que lhes proporciona um ambiente personalizado e interativo.

Uma aplicação específica de NFC apareceu no Japão e desde então foi introduzido no mercado Americano, que permite um telemóvel atuar como um cartão de pagamento NFC ou um terminal de pagamento ou até ambos. Um interessante exemplo desta tecnologia é o *Google Wallet*. Na Tabela 2.1 estão representados vários exemplos de uso de um telemóvel NFC.

Tabela 2.1 - Exemplos de uso de um telemóvel com NFC.

	Estação Aeroporto	Veículo	Escritório	Loja Restaurante	Teatro Estádio
Área					
Uso do telemóvel NFC	Porta de entrada Obter Informação de um smart poster Obter informação de um kiosk de informação Pagar autocarro/taxi	Personalizar a posição do banco Usar como substituição da carta de condução Pagar o parque	Entrar/Sair do escritório Troca de cartões de visita Log in PC; Imprimir usando uma fotocopiadora	Pagamento com cartão de crédito Guardar pontos de lealdade Guardar e usar cupões Partilhar informação e cupões com vários utilizadores	Bilhete de entrada Obter informação do espectáculo
Industrias	Transportes Públicos Publicidade	Fabricantes e prestadores de serviços automóvel	Segurança	Bancos Lojas Cartões de crédito	Entretenimento

2.2. Tecnologia de comunicação

Para efetuar a comunicação NFC foi adotada uma tecnologia de transferência de energia baseada no acoplamento magnético de dois sistemas ressonantes, estabelecendo um *link* de comunicação próximo, um *link* indutivo. Este tipo de ligação cria um campo magnético na proximidade do dispositivo que o gera e não radia para o espaço livre. Na Figura 2.1 está representadas as diferença entre um *link* que propaga para o espaço livre e um *link* indutivo.

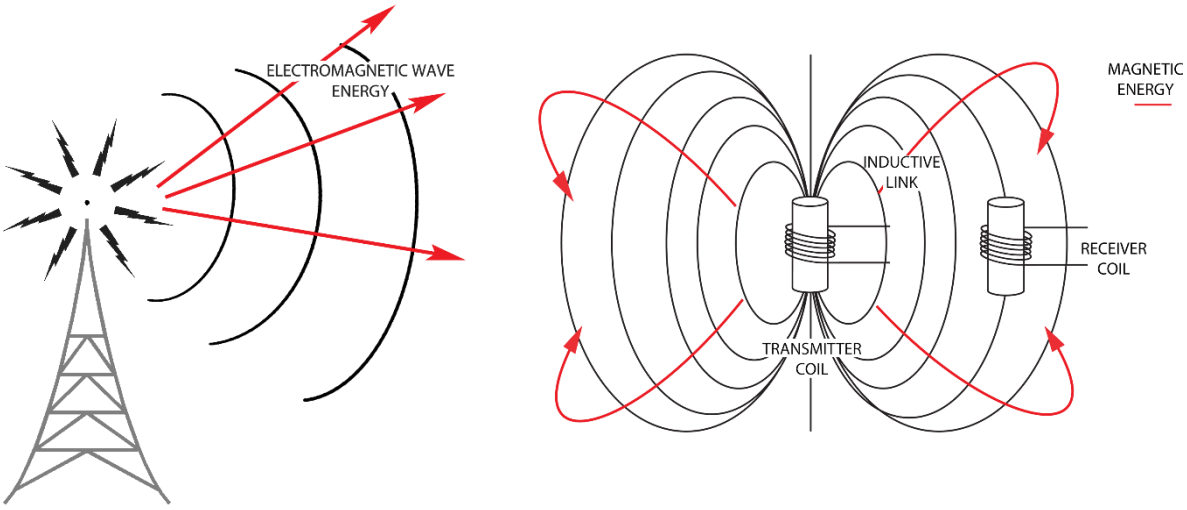


Figura 2.1 - Comunicação usando radiação de longo (*far-field*) e curto alcance (near-field).

No *link* indutivo cada ressoador pode ser representado por um circuito LC ressonante, onde o ressoador primário está ligado a uma fonte de potência e o secundário a uma carga (Figura 2.2). Os dois ressoadores estão acoplados indutivamente para que uma corrente fornecida no primário induza uma corrente no secundário.

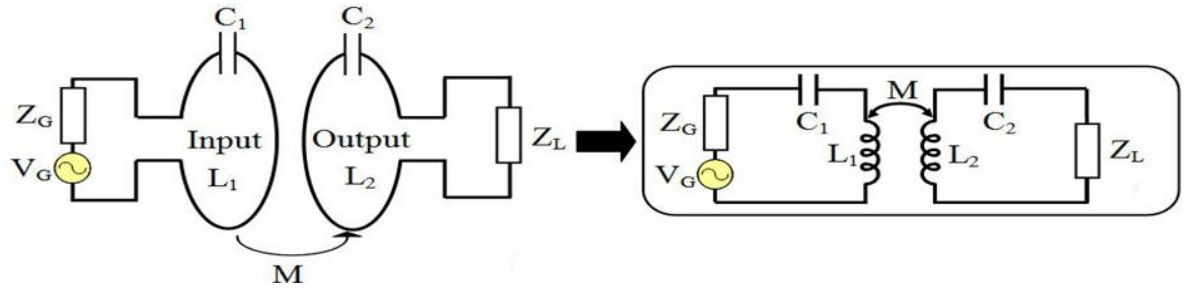


Figura 2.2 - Representação esquemática de um *link* indutivo.

2.3. Modos de operação do NFC

A interface opera em vários modos. Os modos são definidos consoante o dispositivo consiga criar o seu próprio sinal RF ou adquire energia de outro dispositivo para gerar o seu sinal RF. Se o dispositivo gerar o seu próprio sinal é chamado o dispositivo ativo, caso contrário é de caracter passivo. Os dispositivos ativos normalmente estão ligados a uma fonte de alimentação, os passivos, como os cartões sem fios, têm que ser alimentados através do sinal RF de outro dispositivo.

São possíveis 3 modos de comunicação, *peer-to-peer*, *reader/writer*, e *card emulation* [8].

O modo *peer-to-peer* permite a comunicação entre dois dispositivos. O dispositivo que inicia a comunicação é chamado o *initiator* e outro é chamado o *target*. O dispositivo A começa por enviar uma mensagem para o dispositivo B e este retorna uma mensagem de resposta. O B não pode enviar dados nenhuns sem primeiro receber dados do A. O protocolo que suporta a configuração do *initiator* e do target no modo *peer-to-peer* assegura um bom estabelecimento da comunicação e é chamado de *Logical Link Control Protocol (LLCP)*. A principal diferença deste modo é o consumo de energia do *initiator* e do *target*, pois ambos são alimentados para produzir o seu sinal RF [8].

O segundo modo é o *reader/writer* que permite aos dispositivos NFC comunicar com *tags* do NFC Forum. Estas *tags* são normalmente componentes passivos e podem ser inseridas em posters ou outros sítios em que por toque do dispositivo NFC na *tag* a informação nesta gravada é lida pelo dispositivo. Estas podem conter informação como endereços de internet ou executar uma ação no dispositivo tal como ligar a uma rede wireless [8].

O terceiro e último modo é o modo de *card emulation*, que permite a um dispositivo ativo NFC emular um cartão para comunicar com os leitores RFID. O dispositivo pode emular um ou mais RFID *Smart Cards*[1]. Com este modo é possível usar as infraestruturas já existentes tal como as de pagamento e controlo de acessos.

A emulação do *Smart Card* pode ser feita a nível da camada aplicacional ou num elemento seguro em hardware. Um elemento seguro é um dispositivo, similar a um *Smart Card* real que usa uma interface ao dispositivo NFC para transferir os seus dados. Com o combinar do elemento seguro e o modo *reader/writer* é possível implementar uma vertente similar mas mais simples do modo *peer-to-peer*, o que com o hardware correto permite usar o dispositivo NFC quando este está desligado ou com pouca energia. A Figura 2.3 mostra os 3 modos de operação do NFC.

[1] Um *Smart Card* é um cartão normalmente feito em plástico que contém circuitos integrados embebidos, contendo componentes como memória volátil e microprocessador. Estes permitem identificar, autenticar, armazenar dados e correr aplicações.

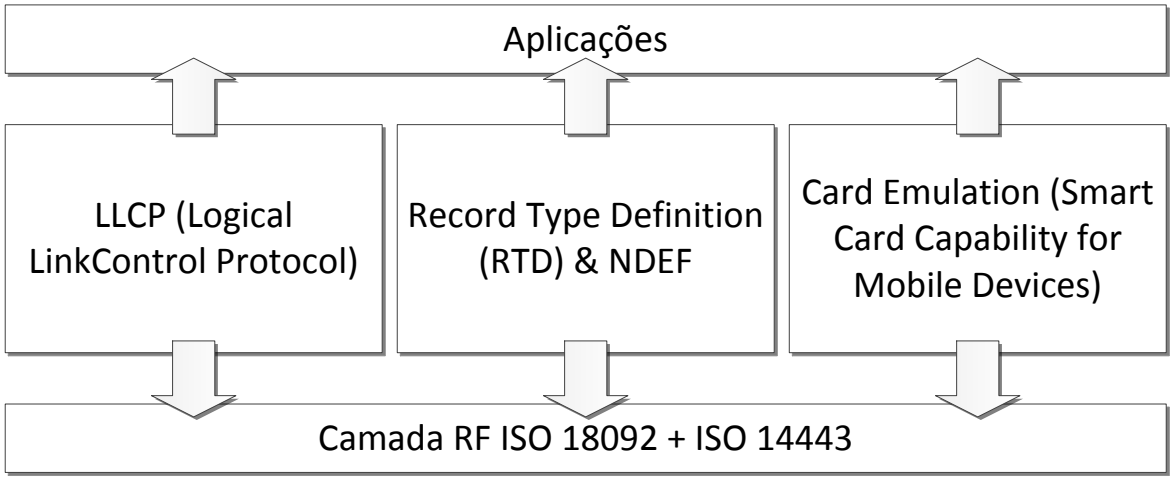


Figura 2.3 - Modos de operação NFC.

A comunicação NFC não está limitada apenas a comunicação entre 2 dispositivos, um dispositivo *initiator* pode comunicar com vários *targets*. No cenário em que todos os dispositivos são ativados ao mesmo tempo o *initiator* seleciona o recetor antes de enviar uma mensagem, a mensagem é ignorada por todos os outros que não foram selecionados. Apenas o *target* selecionado pode responder aos dados recebidos. Em sistemas NFC não é suportado o envio de dados a vários dispositivos ao mesmo tempo (*broadcasting*).

2.4. Arquitetura hardware NFC

A arquitetura do hardware compromete os componentes a nível físico e a interação entre os mesmos. Os principais componentes da arquitetura do hardware do NFC são:

1. O *Host Controller*: O ambiente de execução da aplicação, onde a aplicação está armazenada como por exemplo o telemóvel;
2. O Elemento Seguro: O ambiente de execução seguro, onde a informação delicada como os dados do cartão de débito é armazenada, encontra-se dentro do Elemento Seguro;
3. O Controlador NFC: permite a ligação entre o *Host Controller* e a comunicação NFC, contém uma interface de comunicação com o elemento seguro;
4. Antena NFC: permite a transmissão do sinal RF e é tipicamente feita com *loops* de fios ou pistas quando integrada numa PCB;

Aqui vão ser descritos em detalhe os dois elementos centrais da lista anterior, o Elemento Seguro e o Controlador NFC. A Figura 2.4 mostra os elementos NFC que estão ou podem estar presentes num dispositivo móvel.

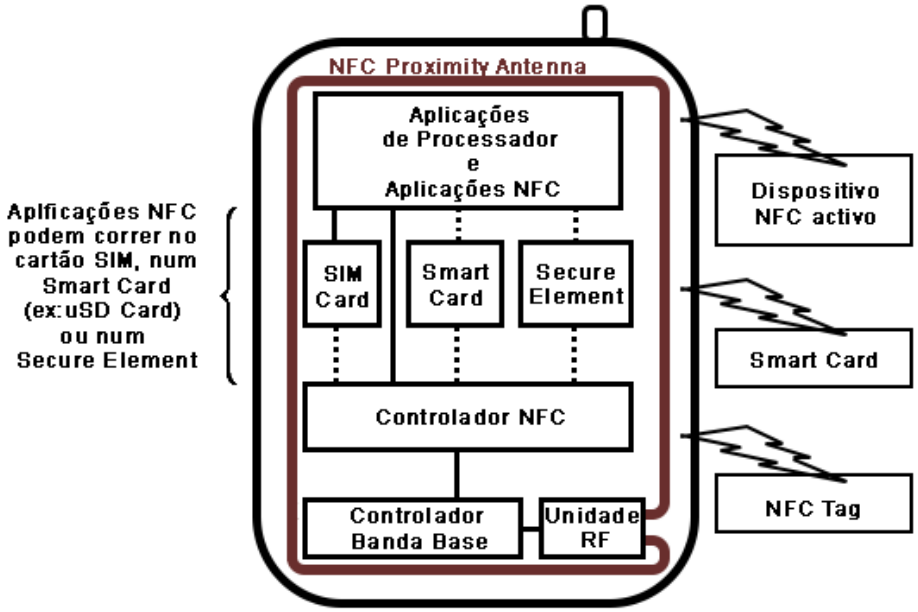


Figura 2.4 - Descrição dos elementos hardware NFC num telemóvel.

2.5. Controlador NFC

O Controlador NFC tem como função reencaminhar os dados que chegam através do sinal RF para o Host Controller e Elemento Seguro. Existem várias interfaces de comunicação entre o Host Controller e o Controlador NFC, como a interface série SPI, UART e USB. Para a comunicação entre o Controlador NFC e o Elemento seguro são usadas interfaces típicas dos *Smat Cards* como a interface NFC Wired (NFC-WI) ou a Single Wire Protocol (SWP). Os Controladors NFC contêm microprocessadores integrados que implementam as camadas de baixo nível da norma NFC.

2.6. Elemento seguro

Na maioria dos dispositivos móveis, tais como os telemóveis, não existe maneira de armazenar dados seguros diretamente. Para a maioria das aplicações NFC, isto é, aplicações de pagamento e de autenticação, um sistema de armazenamento seguro é essencial. Para dados sensíveis, o armazenamento tem que ser resistente à manipulação, tem que

implementar funções de criptografia para executar software com restrições de segurança. Os *Smart Cards* normalmente implementam estes requisitos.
Para implementar estes elementos seguros existem várias possibilidades, cada uma com as suas vantagens e desvantagens:

1. Software sem hardware seguro: O Software é a solução mais flexível, mas sem hardware seguro pode não estar otimamente seguro. Existe sempre a possibilidade do hardware não seguro poder ser manipulado.
2. Hardware seguro integrado: Esta é a solução que coloca maior dependência no hardware mas a mais fiável e segura. O Elemento seguro pode estar incorporado no Host ou ser um chip isolado. O tipo de interface usada para comunicar com o Elemento Seguro é a mesma que é usada para comunicar com um *Smart Card* (SWP) ou então é usada a interface NFC-WI. Com esta solução quando o utilizador mudar de dispositivo a informação tem que ser eliminada do dispositivo antigo e colocada no novo.
3. Hardware removível: na maioria dos casos esta será a melhor solução-compromisso entre a fiabilidade, flexibilidade e custos. Como é necessário uma interface de hardware para colocar o Elemento Seguro removível, os custos de produção do dispositivo serão mais elevados. Os dispositivos removíveis podem ser cartões de memória seguros (SMC), que combinam as funções seguras de um *Smart Card* com a memória de armazenamento habitual que disponibilizam. Outra solução passa por um Universal Integrated Circuit Card (UICC) que nos telemóveis corresponde ao cartão Subscriber Identity Module (SIM).

2.7. Formato de dados NFC

Para garantir a compatibilidade entre todos os dispositivos NFC e RFID, o formato dos dados foram normalizados.

2.7.1. *Tags* do Forum NFC

As *tags* são uma parte importante desta tecnologia. Estas implementam os dispositivos de armazenamento passivo, tais como os *smart-posters*, e estão presentes noutras áreas onde

dados de pequenas dimensões necessitam de ser armazenados e transferidos para os dispositivos ativos. Os dados podem ser lidos das *tag*s passivas com o toque de um dispositivo ativo NFC. Os dados armazenados nas *tag*s podem conter qualquer tipo de dados, mas nas aplicações comuns são usadas para armazenar URL's, onde depois o dispositivo NFC poderá encontrar mais informação.

2.7.2. NDEF (NFC Data Exchange Format)

O formato NFC Data Exchange Format (NDEF) [9] define o formato da mensagem para permitir a comunicação entre dois dispositivos NFC ou entre um dispositivo NFC e uma *tag* do NFC Forum. Este formato garante a consistência das mensagens trocadas entre dispositivos NFC.

2.7.3. Definição do tipo de dados NFC (*NFC Record Types Definition*)

A especificação *NFC Record Types Definition* define o tipo de dados a ser guardado para as aplicações que usam o formato NDEF conhecerem e identificarem a estrutura do conteúdo guardado. Para permitir que outras organizações especifiquem o seu tipo de dados para além dos definidos pelo NFC Forum, existe a classificação *NFC Forum External Types* para além da *NFC Forum Well-Known Types*. A classificação *NFC Forum Well-Known Types* é especificada pelo NFC Forum, que fornece a orientação para processar e representar os dados. Elas são:

- *Text Record Type*: contém texto simples e não tem nenhuma aplicação atribuída;
- *URI Record Type*: contém um *Uniform Resource Identifier* (URI), que pode ser um e-mail, um endereço web, números de telefone ou outros códigos de identificação;
- *Smart Poster Record Type*: é uma extensão do *URI Record Type*, fornece informações adicionais relacionadas com o URI, como ícones ou executar uma aplicação no dispositivo como lançar o *browser* para aceder a um *website*;
- *Generic Control Record Type*: fornece uma maneira de virtualmente pedir para executar uma ação específica como correr uma determinada função ou aplicação no dispositivo de destino;

- *Connection Handover*: fornece *handover* sobre uma conexão NFC para outra tecnologia de comunicação, como o *Bluetooth*.

2.8. NFC e pagamentos com telemóvel (Google Wallet)

Como referido anteriormente, um exemplo interessante de pagamentos com um terminal móvel através de NFC é o Google Wallet. É uma aplicação para os dispositivos Android que permite aos telemóveis interagir com o terminal de pagamento NFC. É compatível com os dispositivos Android mais recentes que suportem pagamentos NFC e também com outros telemóveis que contenham Elementos Seguros integrados ou externos. Uma entidade bancária pode carregar um cartão de pagamento no chip do Elemento Seguro na forma de um *Java Card Applet*, o utilizador pode depois selecionar o cartão através do ecrã do telemóvel e usá-lo para pagar, passando o telemóvel pelo terminal de pagamento numa loja física ou usá-lo numa transação online. A Figura 2.5 mostra uma imagem do processo de pagamento numa loja fazendo uma transação através do Google Wallet [10].

Figura 2.5 – Uso do Google Wallet numa loja.

2.9. Proteção e segurança em NFC

Esta secção discute as medidas de proteção e segurança disponíveis na tecnologia NFC. Inicialmente fala-se um pouco de segurança e privacidade no geral dentro do campo NFC. É feita uma discussão acerca da segurança dos pagamentos NFC com um telemóvel e usa-se o Google Wallet como exemplo.

2.9.1. Generalidades na proteção e segurança NFC

A segurança numa comunicação é a prevenção de acesso e manipulação não autorizados aos dados. A segurança é caracterizada em 3 princípios:

- Confidencialidade, é o princípio onde apenas aqueles com suficientes privilégios podem aceder a determinada informação. Quando a informação pode ser visualizada por pessoal ou um sistema não autorizado, a confidencialidade é quebrada;
- Integridade, é o princípio de garantir que a informação é mantida num estado válido e completo. A integridade da informação é ameaçada quando é exposta a danos, destruição, ou outro método de mudança do seu estado original. A corrupção dos dados pode ser feita quando a informação está a ser inserida, gravada ou transmitida.
- Disponibilidade, é o princípio que permite que entidades acedam à informação num formato útil e sem interferência ou obstrução. Uma entidade pode ser uma pessoa ou um sistema de computadores. Disponibilidade não implica que a informação esteja disponível a qualquer utilizador, pelo contrário a informação apenas está disponível para utilizadores autorizados.

A Figura 2.6 representa como é criada a segurança de um sistema usando os princípios da confidencialidade, integridade e disponibilidade.

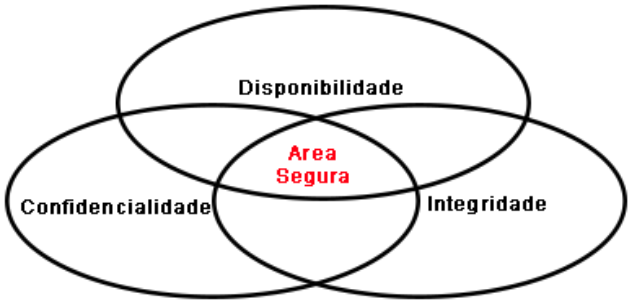


Figura 2.6 - Criação de segurança num sistema.

Existem muitas maneiras de passar pela segurança de um sistema, os três ataques mais comuns são:

- Espionagem: obtém acesso não autorizado à informação;
- Engano: iludir com a informação errada;
- Negação de serviço: sobrecarregar o sistema de maneira a que este se torne inoperável.

Todos os tipos de comunicação sem fios estão vulneráveis a estes ataques. É fácil escutar um canal *wireless* e o sinal pode facilmente ser perturbado por outros sinais. O problema das transmissões rádio é que os utilizadores maliciosos podem aceder ao canal de comunicação sem serem detetados. Sem nenhuma proteção, é possível ver mensagens, alterar a informação em tempo real, guardar a informação e expola mais tarde com o conteúdo original ou alterado. Para se defender dos ataques é necessário que o sistema implemente autenticação, verificação da integridade dos dados e proteção de cópia. O nível de segurança necessário é definido para a aplicação em questão, quando está dinheiro envolvido, a aplicação irá atrair potenciais utilizadores maliciosos. A partilha de conteúdo privado pode não necessitar do mesmo nível de segurança. MasterCard, VISA e outros vendedores de equipamento nesta área, implementam diferentes soluções de segurança neste campo. Algum do trabalho realizado por estas empresas é público, mas especificações técnicas mais específicas são mantidas entre estas e os parceiros de confiança. O modo de comunicação passivo parece ser uma boa solução para transferir dados sensíveis, pois neste modo é mais difícil de escutar comparado com as comunicações de modo ativo [11].

São aqui mostrados três elementos chave de ataques em NFC, ataques através da interface de transmissão (o espaço livre), através de uma *tag* NFC e através do dispositivo NFC.

2.9.2. Ataques através da interface RF

Como resultado da interface ar ser sem contacto, os ataques podem ser feitos sem acesso físico. Isso significa que há inúmeras possibilidades de um ataque ser feito. Os ataques conhecidos através da interface espaço livre são:

- Leitura a grande distância, consiste na alteração de um dispositivo NFC para ler *tags* a uma distância segura. Não é um ataque fácil de efetuar pois a potência do sinal têm

que ser aumentada, usar uma antena otimizada e terá que lidar com o aumento do ruído na comunicação.

- *Jamming*, o ataque é feito enviando um sinal à frequência de comunicação para perturbar o sinal e evitar a comunicação.
- Recusa de serviço, como pode haver mais que um dispositivo NFC/*tag* na proximidade, um algoritmo de anti colisão é executado para selecionar um único dispositivo. O atacante gera colisões/respostas para todos os possíveis endereços de dispositivos e simula a existência de uma grande densidade de dispositivos próximos do leitor. O leitor irá aceder a cada um dos dispositivos para o desativar para conseguir falar com o dispositivo necessário. Mas no caso em que o leitor nunca consegue comunicar com os dispositivos simulados, a comunicação é bloqueada.
- Intermediário indesejado, neste ataque duas partes que pretendem comunicar entre si são levadas para uma comunicação com 3 participantes sem o seu conhecimento. Em vez de comunicarem uma com a outra, comunicam com o terceiro participante que intercepta as mensagens entre estas. Assim é possível mudar os dados antes destes chegarem ao recetor original.
- *Eavesdropping*, devido ao facto dos sistemas NFC comunicarem por ondas eletromagnéticas numa interface aberta, o ar, é possível qualquer recetor próximo escutar a comunicação. Devido ao facto do recetor do atacante ter alimentação própria tem possibilidade de amplificar os sinais fracos recebidos a uma distância de 30 a 40 cm [11] [12]. Em [11] é demonstrado que produzir este equipamento pode ser feito a um baixo custo.
- *Relay attack*, neste ataque o invasor usa outro canal de comunicação como um intermediário para aumentar a distância de comunicação. O atacante não necessita de acesso físico ao dispositivo, apenas de uma antena e o segundo canal de comunicação na área. Do outro lado o equipamento pode estar muito distante, a fazer a emulação do cartão original. O atacante só tem que cumprir os tempos de comunicação especificados na norma. Na Figura 2.7 está representado um possível cenário deste ataque.

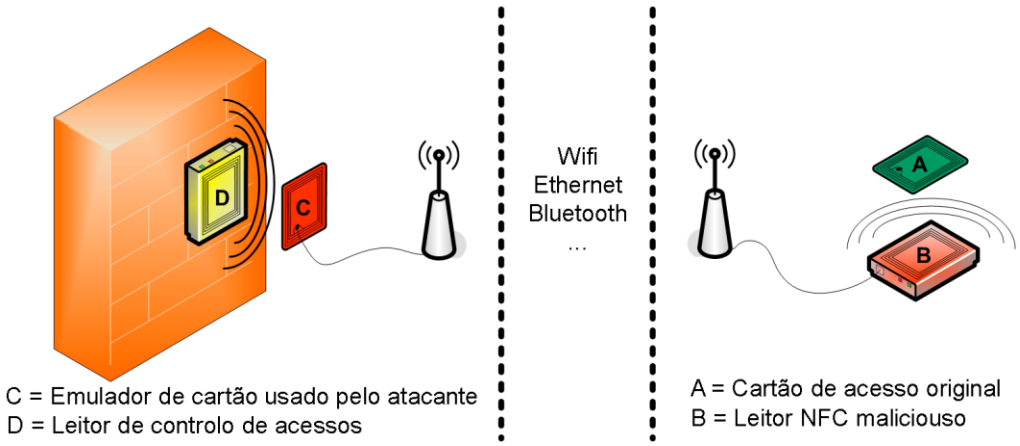


Figura 2.7 - Exemplo de um Relay attack

2.10. Medidas de segurança contra ataques em dispositivos NFC

Desde que os dispositivos NFC têm vindo a ser utilizados para pagamentos e bilhetes, a segurança começou a ser de alta prioridade. Muitos dos ataques listados anteriormente podem ser prevenidos usando autenticação e métodos de encriptação [8]. MIFARE[2] introduziu a norma ISO/IEC 14443 com suporte para os protocolos de encriptação 3DES, AES e RSA [11]. A sua primeira tentativa de implementar segurança foi com o protocolo de encriptação Crypto-1, uma cifra proprietária da NXP com uma chave de 48bits feita para os dispositivos MIFARE Classic. Devido ao seu baixo custo e segurança, esta versão foi massivamente usada em carteiras eletrónicas, transportes públicos e bilheteiras. Algumas publicações em 2007 e 2008 descrevem como quebrar esta cifra, uma delas em 40*ms* [13]. As últimas soluções da MIFARE e FeliCa são aprovadas no nível de segurança EAL4 definido pelo organismo internacional *Common Criteria* que está especificado na norma ISO/IEC 15408. O nível EAL4 é o nível mais alto em que é expectável ser economicamente rentável quando implementado num produto. O nível de segurança EAL5 tem um processo de desenvolvimento rigoroso e é aplicável em sistemas que necessitem ter assegurado um alto nível de segurança. O hardware SmartMX da MIFARE passou o nível EAL5+. O fabricante da marca FeliCa implementou num dos seus produtos o método de encriptação 3DES em que

[2] MIFARE é uma marca adquirida pela NXP Semiconductors de uma série de chips muito usada em *Smartcards* sem contacto.

as chaves são partilhadas no processo de autenticação, o fabricante garante na descrição do produto que é praticamente impossível falsificar e quebrar a segurança dos cartões com esta tecnologia de encriptação [14].

2.11. Proteção e segurança nos sistemas de pagamento NFC

Desenvolver um sistema de pagamentos NFC é um desafio, pois o sistema será usado por centenas de milhares de utilizadores, bancos e vendedores, cada um querendo baixar os custos e adaptar aos seus próprios sistemas podendo prejudicar a segurança. Uma desvantagem dos pagamentos via NFC é que os crimes que antes eram difíceis de executar nos tradicionais sistema de pagamentos com chips e dispositivos com pinos, de repente se tornam viáveis. No presente é possível ligar um terminal tradicional com chip falso a um cartão tradicional falso remotamente, e enquanto a vítima paga um café na máquina de cafés onde terminal falso foi instalado, do outro lado a quilómetros de distância o criminoso pode levantar o dinheiro numa ATM com um cartão falso.

3. Desenvolvimento

3.1. Enquadramento

Este projeto de mestrado permite identificar um utilizador de uma estrada concessionada para posterior cobrança do percurso efetuado, sendo uma alternativa ao pagamento manual (numerário e cartão) ou automático existente nas vias de hoje em dia. Na Figura 3.1 está representada a visão geral do sistema de identificação por NFC. É constituído por 3 elementos principais, o telemóvel, o leitor NFC e o servidor de autenticação que têm as seguintes funções:

- Telemóvel – telemóvel com tecnologia NFC que comunica com o Leitor NFC e envia os dados de identificação para o leitor. Após identificação bem sucedida, apresenta no ecrã o valor e o percurso percorrido, guardando os dados no histórico.
- Leitor NFC – leitor com uma antena adaptada para comunicar nos 13.56MHz que faz a desmodulação do sinal RF e implementa as normas de baixo nível da norma NFC. Tem associado um processador para gerir as comunicações, comunicar com o servidor de autenticação e dar informação ao utilizador num ecrã.
- Servidor de autenticação – servidor que recebe os dados do telemóvel validando a sua identificação para autorizar ou recusar a sua passagem na portagem.

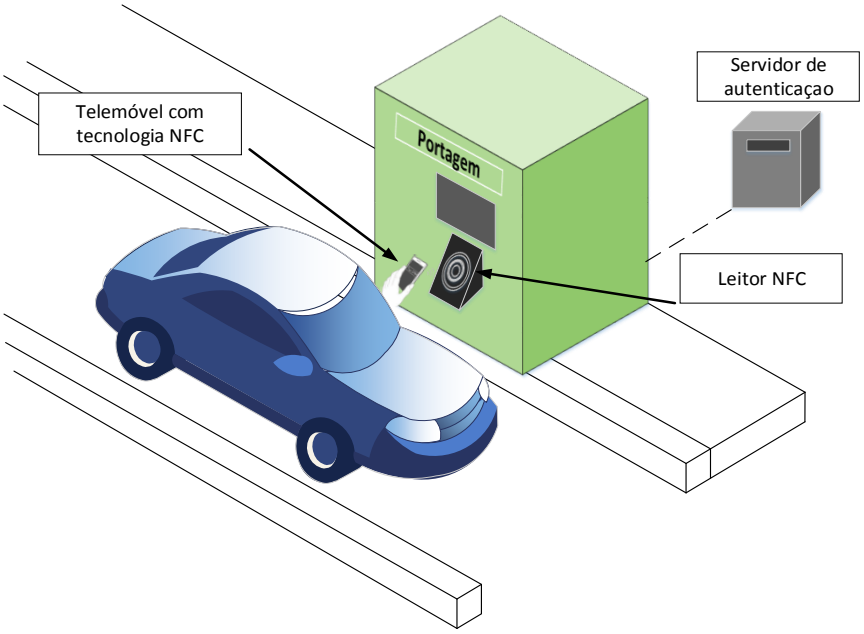


Figura 3.1 – Visão geral do sistema de identificação NFC.

3.2. *Transceiver* NFC

Para implementar o sistema de identificação NFC foi necessário selecionar um sistema de comunicações já integrado que implementasse a camada RF a 13.56 MHz assim como algumas camadas de baixo nível existentes na norma. Foi escolhido o chip integrado PN532 da NXP.

3.2.1. Introdução ao controlador NFC PN532

O PN532 é um *transceiver* integrado para comunicações a 13.56 MHz baseado no core do microcontrolador 80C51 e suporta as seguintes funcionalidades:

- ISO/IEC 14443A/MIFARE Reader/Writer
- FeliCa Reader/Writer
- ISO/IEC 14443B Reader/Writer
- Emulação de cartões ISO/IEC 14443A/MIFARE, MIFARE 1 KB ou MIFARE 4 KB
- Emulação de cartões FeliCa
- ISO/IEC 18092, ECMA 340 Peer-to-Peer

O PN532 implementa um desmodulador e descodificador para comunicar com dispositivos que implementam a norma ISO/IEC 14443A/MIFARE, ISO/IEC 14443 B, FeliCa e ISO/IEC 18092 NFCIP-1 em modo passivo e ativo. O integrado executa por completo a descodificação das tramas das várias normas, fazendo a deteção de erros (Paridade e CRC), este permite velocidades de transferência de dados até 424 kbit/s em ambas as direções. Apenas é possível emular um cartão com completa funcionalidade de segurança se ligar um elemento seguro ao integrado através da interface NFC-WI/S2C.O PN532 pode ser ligado a uma antena externa sem adição de nenhum componente ativo.

Este integrado suporta 3 tipos de interface série para comunicação com o controlador (Host), I2C, SPI e High Speed UART (HSU).

Na Figura 3.2 está representada toda a unidade que implementa a desmodulação e descodificação do sinal RF recebido, bem como os blocos de deteção e correção de erros. Todos estes blocos são controlados por um core 80C51 interno ao PN532 que serve se intermediário entre o exterior (*Host*) e os blocos, para configurar, enviar e receber informação.

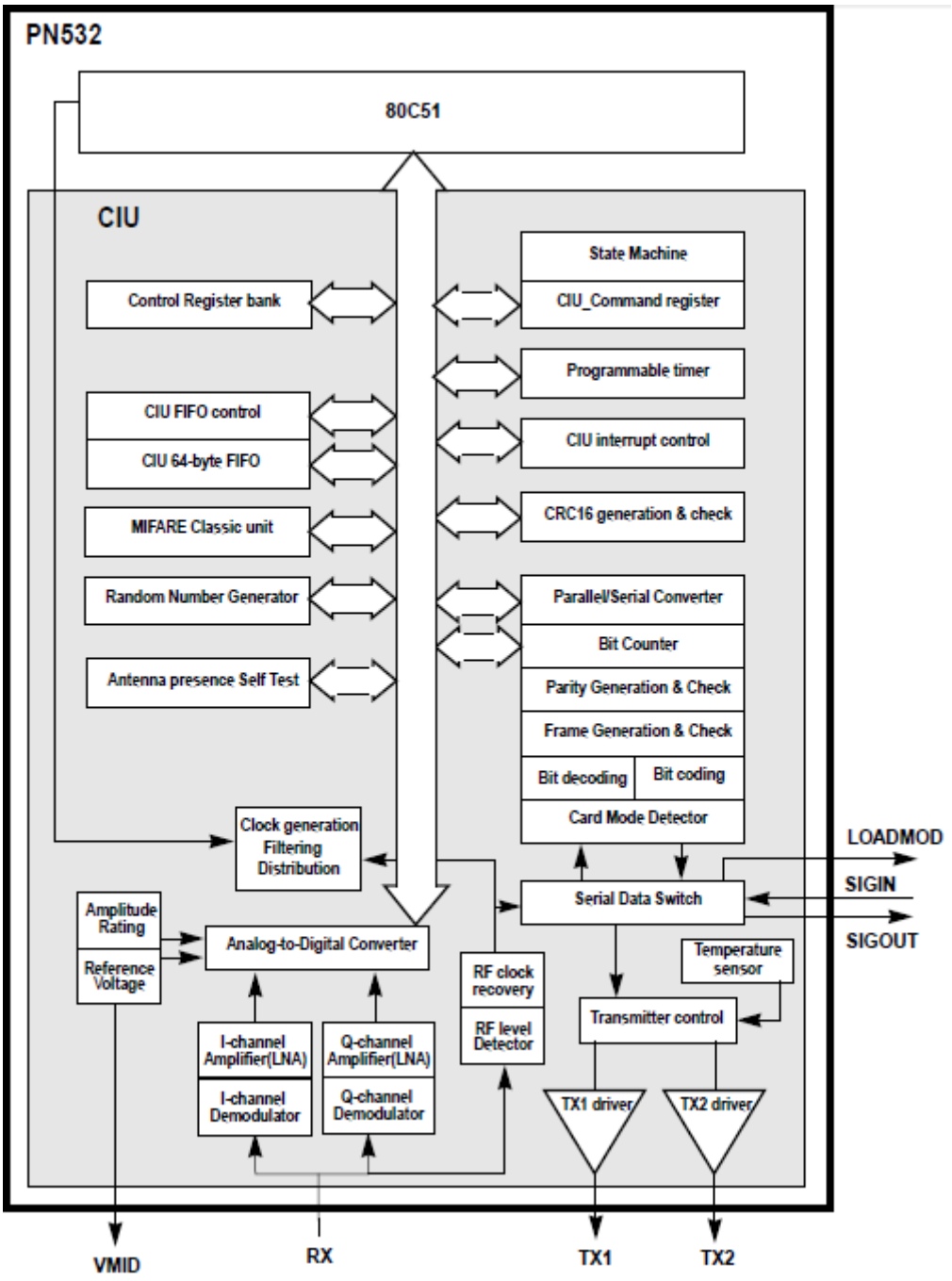


Figura 3.2 - Diagrama detalhado do desmodulador e descodificador do PN532.

3.2.2. Sistema completo de comunicações

Para ter um sistema de comunicações NFC completo funcional utilizou-se uma placa de desenvolvimento que já contém o circuito da Figura 3.3 implementado. A placa contém uma antena em forma de espira, respetiva malha de adaptação ao *transceiver* RF do PN532 e um

cristal externo de 27.12 MHz usado como referência de relógio para o processador interno e para gerar a portadora RF a 13.56MHz.

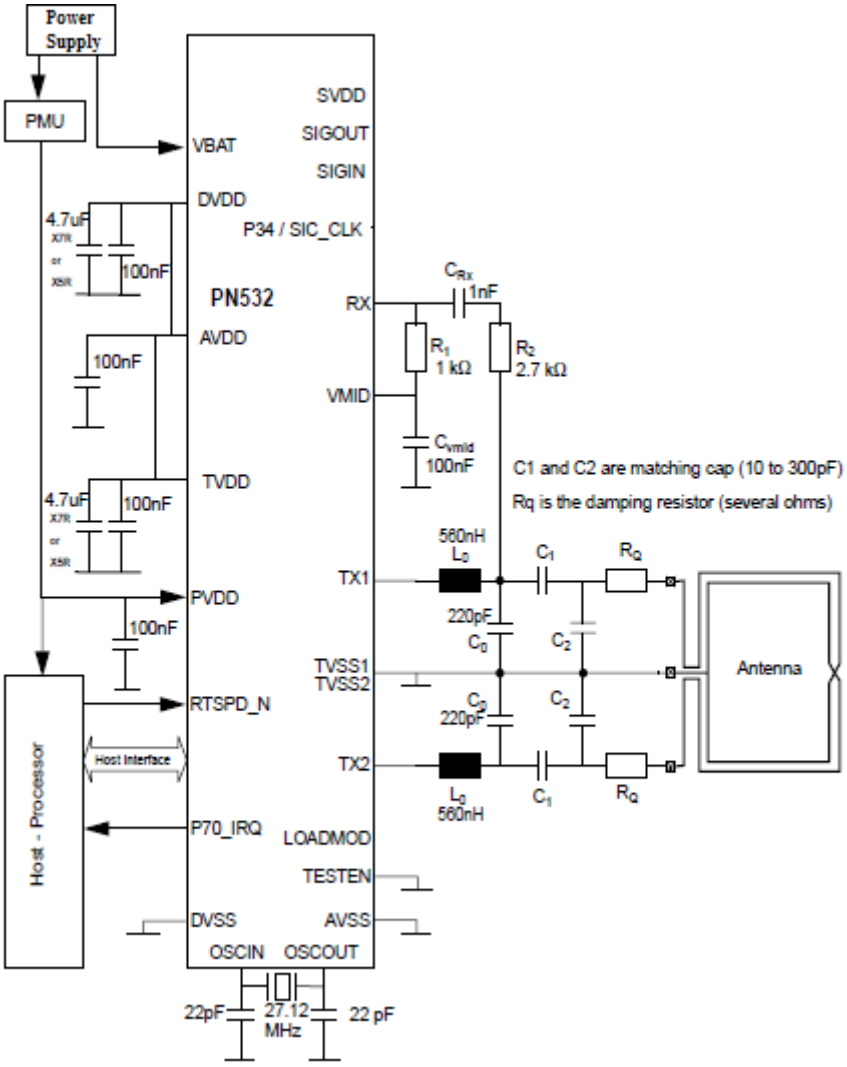


Figura 3.3 - Circuito PN532.

3.3. Processador de controlo (*Host*) e de interface com o utilizador

Para implementar as normas das camadas superiores foi utilizado o sistema embebido *Raspberry Pi* a correr um sistema operativo Linux, usando a biblioteca *Open Source libnfc* para implementar a comunicação com o integrado PN532. Esta biblioteca já contém os comandos apropriados para configurar o PN532, selecionar o modo de comunicação

pretendido (Altivo ou Passivo), configurar os débitos de receção/transmissão, troca de ID's, etc.

3.4. Protocolo de comunicação NFC

Para comunicar com um sistema Android existem dois caminhos possíveis, ou usamos o protocolo de comunicação LLCP (*peer-to-peer*) ou se emula o protocolo de uma *tag* compatível. Para escolher a melhor abordagem estudou-se as duas alternativas.

3.4.1. LLCP (*peer-to-peer*)

O protocolo LLCP foi desenvolvido pelo grupo NFC-Forum [15] e define a segunda camada do modelo OSI para suportar uma comunicação *peer-to-peer* entre dois dispositivos que contenham NFC, sendo essencial para aplicações NFC que impliquem comunicação bidirecional. A especificação define dois tipos de serviço, *connectionless* e *connection-oriented*. O serviço *connectioless* não oferece garantia de fiabilidade ou de controlo de fluxo, reencaminhando estas funções para a aplicação e tirando partido das garantias oferecidas pela camada abaixo, ISO/IEC 18092 [16]. O serviço *connection-oriented* adiciona fiabilidade na entrega das mensagens e controlo de fluxo. Na Figura 3.4 está representado pelo caminho a vermelho as camadas que é necessário implementar para usar o protocolo LLCP.

LLCP é um protocolo compacto, baseado na especificação IEEE 802.2, desenhado para suportar pequenas aplicações com transporte de dados limitado, tal como pequenas transferências de ficheiros.

Para implementação deste protocolo existe como ponto de partida uma biblioteca *open source* denominada de *Libllcp* [17], que nos permite implementar uma comunicação ponto a ponto e receber e enviar mensagens.

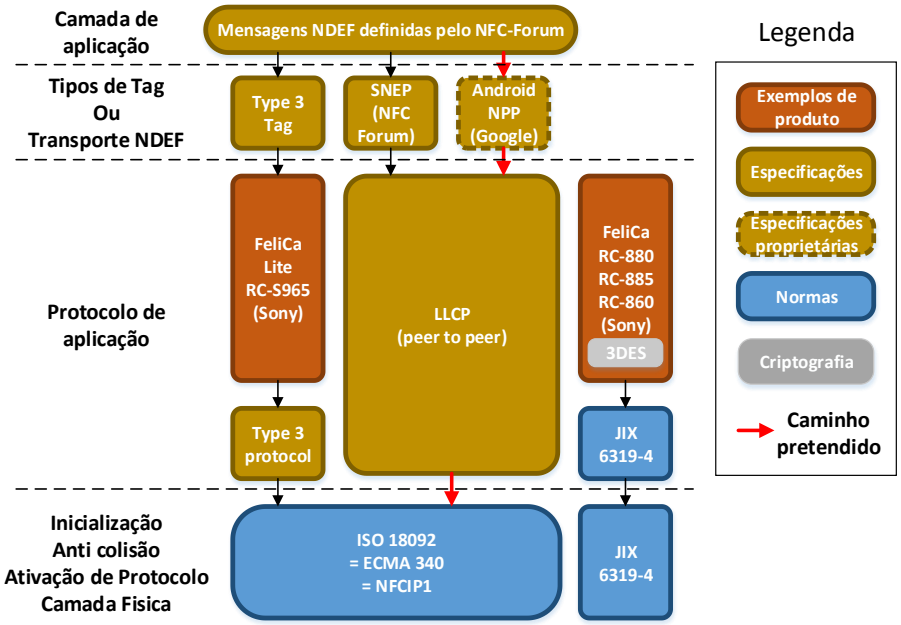


Figura 3.4 - Camadas da comunicação NFC.

3.4.2. Android e protocolo LLCP

O sistema operativo Android oferece uma API a muito alto nível para enviar mensagens NDEF através do protocolo LLCP chamada de Android Beam [18]. O sistema operativo quando inicia a comunicação com um dispositivo NFC compatível envia um evento à aplicação, permitindo a esta a receção e envio de mensagens NDEF, com a particularidade de o envio das mensagens requererem a autorização do utilizador, através de um pedido externo à aplicação enviado pelo sistema operativo que coloca a aplicação em segundo plano, Figura 3.5. Sendo uma necessidade deste sistema o envio de várias mensagens ao leitor, este tipo de limitação compromete a flexibilidade e facilidade de uso da aplicação no telemóvel comprometendo assim o uso deste sistema para troca de mensagens via NFC. Devido a este facto avançou-se com o estudo da segunda opção.

Figura 3.5 - Pedido externo da API do Beam.

3.4.3. Emulação de *tag*

A emulação de *tag* passa por simular uma representação virtual exata de um cartão passivo existente no mercado usando apenas software. A emulação por software implica cumprir os tempos de resposta que antes eram implementados por hardware dedicado, o que pode ser de difícil implementação. Por outro lado o facto de se virtualizar o cartão em software oferece a flexibilidade de alterar o seu próprio conteúdo sem que seja estimulado externamente por outro dispositivo, tornando este método uma via de troca de mensagens NDEF.

3.4.4. Android e interação com *tags*

O sistema operativo Android oferece uma API para escrever e ler o conteúdo de vários tipos de *tag*, cobrindo a maior parte das *tags* existentes no mercado, a lista de compatibilidade com Android está representada na Tabela 3.1.

Tabela 3.1 – *Tags* compatíveis com sistema Android.

Tipo de *tag*	Especificação
NfcA	ISO 14443-3A
NfcB	ISO 14443-3B
NfcF	JIS 6319-4
NfcV	ISO 15693
IsoDep	ISO 14443-4
Ndef	NFC Forum Type 1,2,3,4 *Tag*
NdefFormatable	*Tag*s NDEF Formatable

Para emulação de uma *tag* foi utilizado a especificação *NFC Forum Type 4 Tag* [19], esta permite ler e escrever para a *tag* através de alguns comandos definidos na norma ISO/IEC 7816-4 [20].

3.4.5. NFC Forum Type 4 Tag

A *tag* de tipo 4 disponibiliza um sistema de ficheiros flexível, incluindo verificação da integridade dos dados e opções de encriptação. Suporta os comandos (APDU) da norma ISO/IEC 7816-4 utilizados pelos cartões MIFARE DESFire EV1 [21], e alguns comandos da mesma norma que permitem selecionar, ler e escrever no ficheiro. Este tipo de *tag* é totalmente compatível com os protocolos das normas ISO-14443A e ISO-14443B usados pelos integrados presentes nos telemóveis e pelo PN532. Na Figura 3.6 está representado o *stack* de camadas usado pela *tag* de tipo 4, bem como alguns exemplos de produtos que usam o mesmo *stack*.

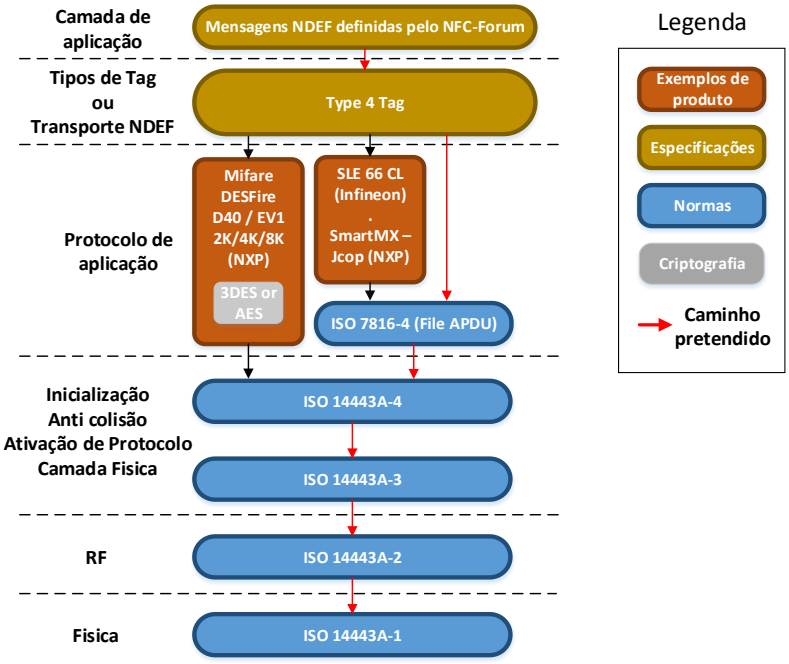


Figura 3.6 - Stack de camadas usadas pela *tag* de tipo 4.

Este tipo de *tag* usa um sistema de ficheiros composto por pelo menos dois ficheiros, o *Capability Container* (CC) e o NDEF. O ficheiro CC contém campos para definir o seu tamanho, versão de mapeamento, tamanhos máximos na troca de dados e um campo que identifica o ficheiro NDEF.

Ficheiro Capability Container (CC)

A Tabela 3.2 contém a descrição de todos os campos que o ficheiro CC contém e a Tabela 3.3 a constituição do bloco TLV.

Tabela 3.2 - Estrutura de dados do ficheiro CC [19].

Offset [bytes]	Tamanho [bytes]	Campo	Descrição
0000h	2	CCLEN [bytes]	Indica o tamanho deste ficheiro CC (incluindo este campo).
0002h	1	Mapping Version	Indica a versão da especificação de mapeamento da qual é compatível.
0003h	2	MLe [bytes]; Maximum R-APDU data size	Define o tamanho máximo dos dados que podem ser lidos da *tag* usando um único comando de READ BINARY.
0005h	2	MLc [bytes]; Maximum C-APDU data size	Define o tamanho máximo dos dados que podem ser enviados para a *tag* através de um comando UPDATE BINARY
0007h	8	NDEF File Control TLV	Bloco TLV que contém informação para controlar e manipular o ficheiro NDEF
000Fh	-	TLV Blocks	Zero, um ou mais blocos TLV começam no offset Fh.

Tabela 3.3 - Constituição do bloco TVL.

Tamanho [bytes]	Campo	Descrição
1	T	Identifica o tipo do bloco TLV e consiste num número entre 00h-FEh.
1 ou 3	L	Tamanho em bytes do campo V, pode ser composto por 1 ou 3 bytes. Este codifica o tamanho do campo V entre 00h-FEh, caso contenha o valor FFh significa que o tamanho do campo V vem nos 2 bytes seguintes.
-	V	Contém dados dependendo do tipo presente no campo T

Tabela 3.4 - Exemplo de conteúdo de um ficheiro CC.

Offset	Tamanho [bytes]	Valor	Conteúdo	
0h	2	000Fh	CCLEN (15 bytes)	
2h	1	20h	Versão de mapeamento 2.0	
3h	2	003Bh	MLe (49 bytes); Tamanho máximo dos dados enviados num trama R-APDU	
5h	2	0034h	MLc (52 bytes); Tamanho máximo dos dados enviados num trama C-APDU	
7h	1	04h	Campo T do bloco TLV de controlo do ficheiro NDEF	
8h	1	06h	Campo L do bloco TLV de controlo do ficheiro NDEF	
9h	2	E104h	Campo V do bloco TLV de controlo do ficheiro NDEF	Identificador de ficheiro
Bh	2	0032h		Tamanho máximo do ficheiro NDEF (50 bytes)
Ch	1	00h		Restrições de leitura do ficheiro NDEF; sem restrições
Dh	1	00h		Restrições de escrita do ficheiro NDEF; sem restrições

Ficheiro NDEF

O ficheiro NDEF é constituído por dois campos, um deles indica o tamanho da mensagem NDEF e o outro contém a própria mensagem. Na Tabela 3.5 está representada a constituição do ficheiro NDEF.

Tabela 3.5 - Constituição de um ficheiro NDEF.

Offset (bytes)	Tamanho (bytes)	Campo	Descrição
0000h	2	NLEN (bytes)	Indica o tamanho da mensagem NDEF armazenada no ficheiro NDEF.
0002h	x	NDEF message	Mensagem NDEF

3.4.6. Comandos de leitura e escrita na *tag*

A *tag* de tipo 4 suporta três tipos de comandos, Select, ReadBinary e UpdateBinary. O comando Select permite selecionar o ficheiro que se pretende ler ou escrever, o ReadBinary serve para ler o conteúdo do ficheiro selecionado e o UpdateBinary para realizar operações de escrita no ficheiro. A comunicação é baseada na troca de 2 tipos de tramas, as Command Application Protocol Data Unit (C-APDU) e as Response Application Protocol Data Unit (R-APDU).

C-APDU

As tramas do tipo C-APDU são enviadas por parte do elemento *Master* da comunicação, neste caso o telemóvel. É na C-APDU que são enviados os comandos Select, ReadBinary e UpdateBinary. O formato da trama C-APDU está representado na Tabela 3.6.

Tabela 3.6 - Formato da C-APDU.

CLA	INS	P1	P2	Lc (opt)	Data (opt)	Le (opt)
Classe	Instrução	Parâmetro byte 1	Parâmetro byte 2	Campo Lc	Dados (Lc bytes)	Campo Le

Os campos que a constituem a C-APDU têm o seguinte significado:

- CLA (1 byte) – Byte que define a classe da C-APDU;
- INS (1 byte) – Define se a instrução é Select, ReadBinary ou UpdateBinary;
- P1 (1 byte) – Parâmetro 1 associado à instrução;
- P2 (1 byte) – Parâmetro 2 associado à instrução;
- Lc (1 byte) – Tamanho do campo Data, opcional;
- Data (Lc bytes) – Dados, opcional;
- Le (1 byte) – Numero de bytes esperados na resposta de uma R-APDU, opcional.

R-APDU

As tramas do tipo R-APDU são as tramas enviadas por parte da *tag*, neste caso o leitor que interage com o telemóvel. Nestas tramas são enviadas respostas com o *feedback* de comandos recebidos de tramas C-APDU enviadas pelo dispositivo *Master*. O formato da trama R-APDU está representado na Tabela 3.7.

Tabela 3.7 - Formato da R-APDU.

Corpo de resposta (opt)	SW1	SW2
Dados	Estado 1	Estado 2

Os campos que a constituem a R-APDU têm o seguinte significado:

- Corpo de resposta (opcional) – transporta os dados da trama R-APDU;
- Bytes de estado SW1 e SW2 – Estado da resposta.

3.5. Troca de dados entre leitor e telemóvel

A troca de dados entre leitor e telemóvel deve ser transparente às restrições impostas pela *tag* de tipo 4 e pela API do Android. Assim este subcapítulo mostra como está estruturada a camada que abstrai a aplicação das restrições de comunicação impostas pelos dispositivos.

Restrições da API NFC do Android para escrita e leitura em tags do tipo 4

O sistema operativo Android quando tem as comunicações NFC ativas funciona como *Initiator* e está sempre a fazer *polling* para encontrar um dispositivo que lhe responda (neste caso o leitor). Ao encontrar o dispositivo lê a mensagem que este envia, e lança um evento na aplicação com o conteúdo lido e o tipo de dispositivo encontrado. A API do Android apenas permite fazer uma leitura e uma escrita por cada evento gerado pelo sistema operativo e para fazer uma escrita implica fazer uma leitura, ou seja por cada mensagem enviada e recebida o leitor NFC tem que ser desativado e novamente ativado para o telemóvel voltar a encontrar um dispositivo e gerar outro evento na aplicação. No diagrama da Figura 3.7 está representado o modo de funcionamento da API do Android para *tags* do tipo 4, onde se pode ver que para voltar a enviar e receber outra mensagem é necessário que o leitor saia da proximidade do telemóvel.

Para contornar esta restrição, o leitor tem que desligar o sinal RF e voltar a ligar para simular uma saída da proximidade do telemóvel.

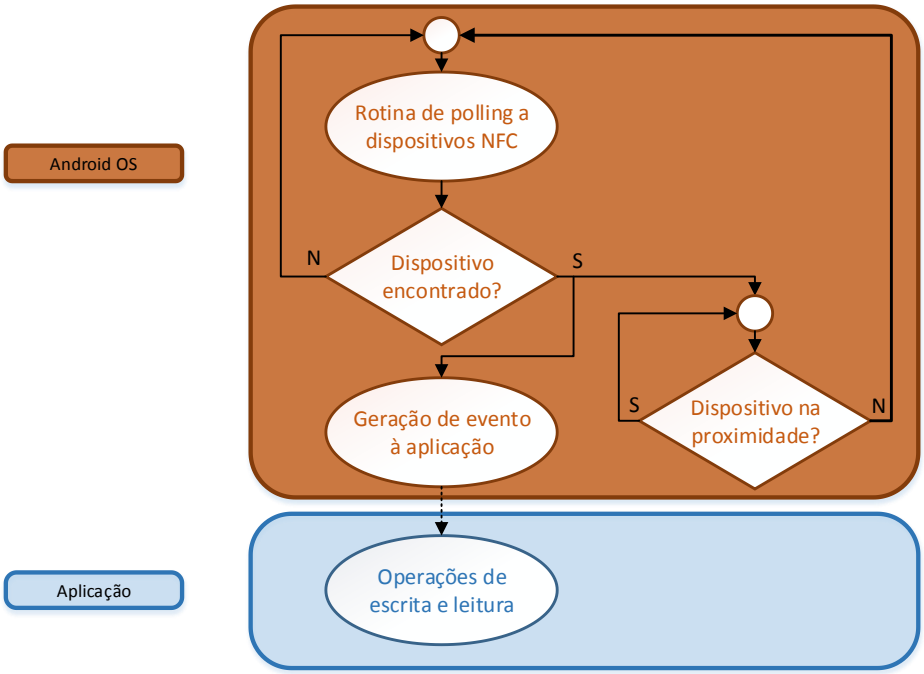


Figura 3.7 - Modo funcionamento da API NFC para *tags* do tipo 4.

3.6. Leitor NFC

O leitor NFC é constituído pelo *transceiver* NFC PN532 descrito em 3.2 e pelo processador *Raspberry Pi* descrito em 3.3. A aplicação desenvolvida para controlar o *transceiver* e abstrair as camadas superiores das restrições de leitura e escrita está representada na Figura 3.8.

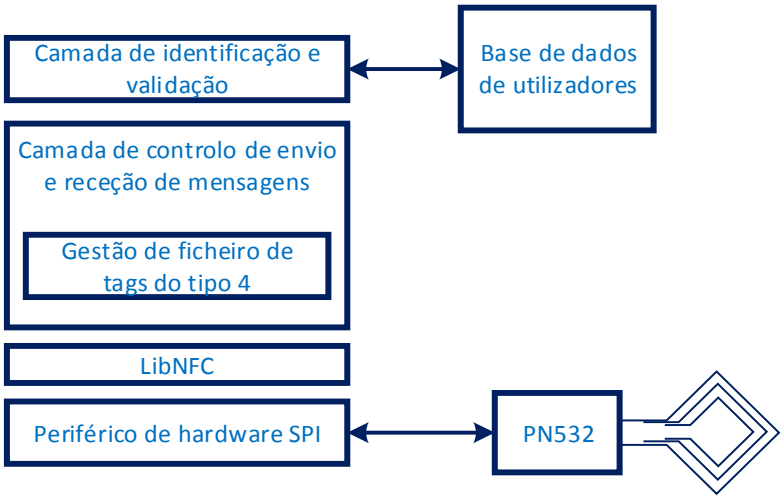


Figura 3.8 - Estrutura de funcionamento do leitor NFC.

O leitor foi desenvolvido em cima da biblioteca LibNFC que implementa a camada ISO/IEC 14443 A/B, e que comunica através do protocolo SPI com o PN532 para enviar e receber dados/comandos. O PN532 implementa também a camada ISO/IEC 14443A/MIFARE mas a parte do protocolo que seria impraticável resolver em software, como a deteção de trama e de erros (Paridade e CRC).

3.6.1. PN532 ISO/IEC 14443A/MIFARE operação em modo de cartão

Ao operar em modo de cartão todas as características do cartão têm que ser emuladas. As modulações, as sub-modulações e os ritmos de transmissão têm que ser de acordo com a primeira coluna da Tabela 3.8. No caso do leitor, este usa para transmitir os dados uma modulação de 100% ASK em conjunto com um código de Miller modificado, enquanto o PN532 que está em modo de emulação de cartão usa uma sub-modulação para a transmissão, o diagrama de comunicação está representado na Figura 3.9.

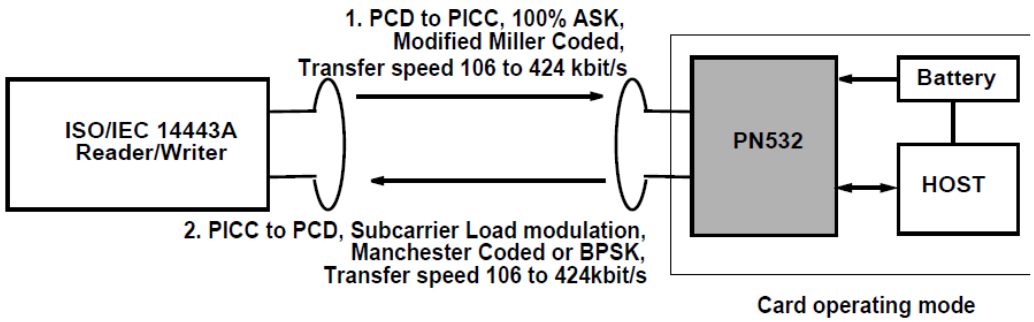


Figura 3.9 - Diagrama do modo de operação de cartão ISO/IEC 14443A/MIFARE.

Tabela 3.8 - Características da operação em modo de cartão ISO/IEC 14443A/MIFARE.

Esquema de comunicação		**ISO/IEC 14443A MIFARE**	**MIFARE débitos mais altos**	
Baud rate		106kbit/s	212kbit/s	424kbit/s
Tempo de bit		$\frac{128}{13.56MHz} = 9.44\mu s$	$\frac{64}{13.56MHz} = 9.44\mu s$	$\frac{32}{13.56MHz} = 9.44\mu s$
Reader/Writer to PN532	Modulação	100% ASK		
	Codificação de bit	Código de Miller modificado		
PN532 to Reader/Writer	Modulação	Sub-modulação de carga		
	Frequência da sub-portadora	$13.56MHz/16$		
	Codificação de bit	Codigo de Manchester	BPSK	

A sub-modulação está localizada a $13.56MHz \pm \frac{13.56MHz}{16}$ como representado na Figura 3.10.

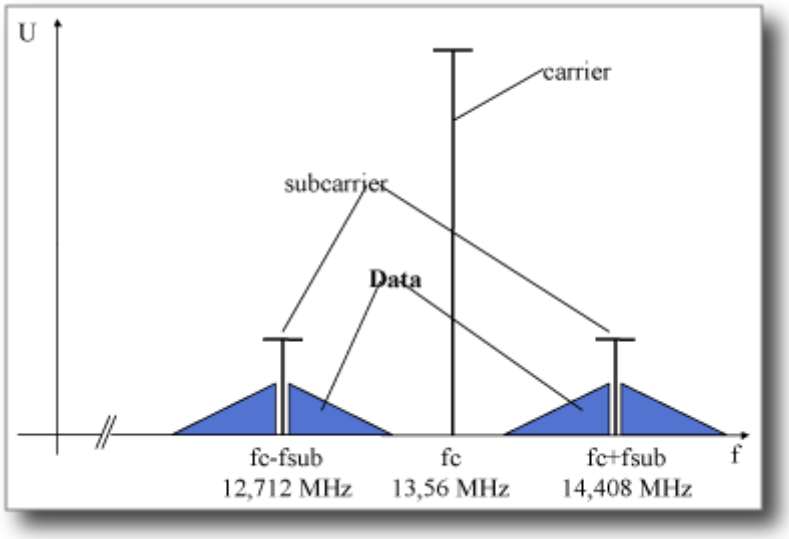


Figura 3.10 - Espectro gerado pelo PN532 no modo de modulação de carga com uma sub-portadora de acordo com ISO/IEC 14443-2.

No caso da comunicação ser passiva (cartão sem alimentação), este tira partido da portadora gerada pelo elemento ativo (telemóvel) e multiplica-a por uma sub-portadora usando uma técnica de modulação de carga que consiste em ligar e desligar uma resistência em paralelo com a antena, no caso de um sistema ativo a portadora é gerada localmente. Na Figura 3.11 está representado um modulador ASK (Amplitude-shift keying) de um elemento ativo bem como o sinal gerado à sua saída e está representado também o sinal caso fosse um elemento passivo. Note-se que no caso de um elemento passivo a portadora de 13.56MHz está sempre presente enquanto no elemento ativo só é gerada quando necessário. Neste projeto do lado do leitor, o PN532 usa uma modulação do tipo ativo.

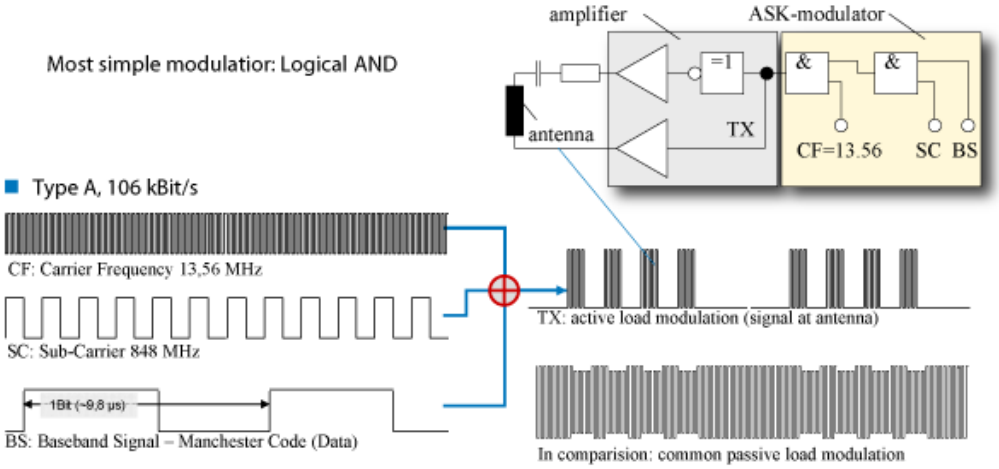


Figura 3.11 - Modulador ASK para gerar uma modulação de um elemento ativo.

3.6.2. LibNFC

A biblioteca *open source* LibNFC é a primeira biblioteca livre de baixo nível lançada compatível com vários sistemas operativos, incluindo GNU/Linux, Mac OS X e Windows. Tem suporte para vários dispositivos de hardware NFC e suporta as normas ISO/IEC 14443 A/B, FeliCa, Jewel/Topaz e *Peer-to-Peer* como *target* e *initiator*. Neste projeto será usada em ambiente Linux e a parte ISO/IEC 14443 A da biblioteca.
As seguintes funções serão usadas para implementar o leitor NFC:

- nfc_target_init( ), esta função define o UID do PN532, configura-o para atuar como *target* e fica à escuta durante um tempo definido. Retorna *timeout* ou sucesso quando um dispositivo *initiator* estiver nas proximidades do leitor;
- nfc_target_send_bytes( ), envia uma sequência de bytes genérica para o *initiator*, pode retornar sucesso, *timeout* ou código de erro;
- nfc_target_receive_bytes( ), recebe uma sequência de dados proveniente do dispositivo *initiator*. Retorna a quantidade de dados recebida, *timeout* ou um código de erro.

3.6.3. Camada de controlo de envio e receção de mensagens

Esta camada foi desenvolvida com o objetivo de abstrair a camada de identificação e validação das limitações inerentes de comunicar com um sistema Android descritos em 3.5. Criou-se duas funções, uma que envia bytes para o telemóvel e outra que recebe os bytes enviados pelo mesmo. Internamente as funções fazem a gestão do momento em que têm que desativar o leitor para simular uma saída da proximidade do telemóvel. Como descrito em 3.5, cada vez que o telemóvel deteta um dispositivo *tag* do tipo 4 é possível realizar uma única operação de escrita e leitura. Assim quando é chamada a função para enviar uma nova mensagem o leitor tem que ser desativado e novamente ativado. No diagrama da Figura 3.12 está representado a gestão que é feita para o envio e receção de mensagens.

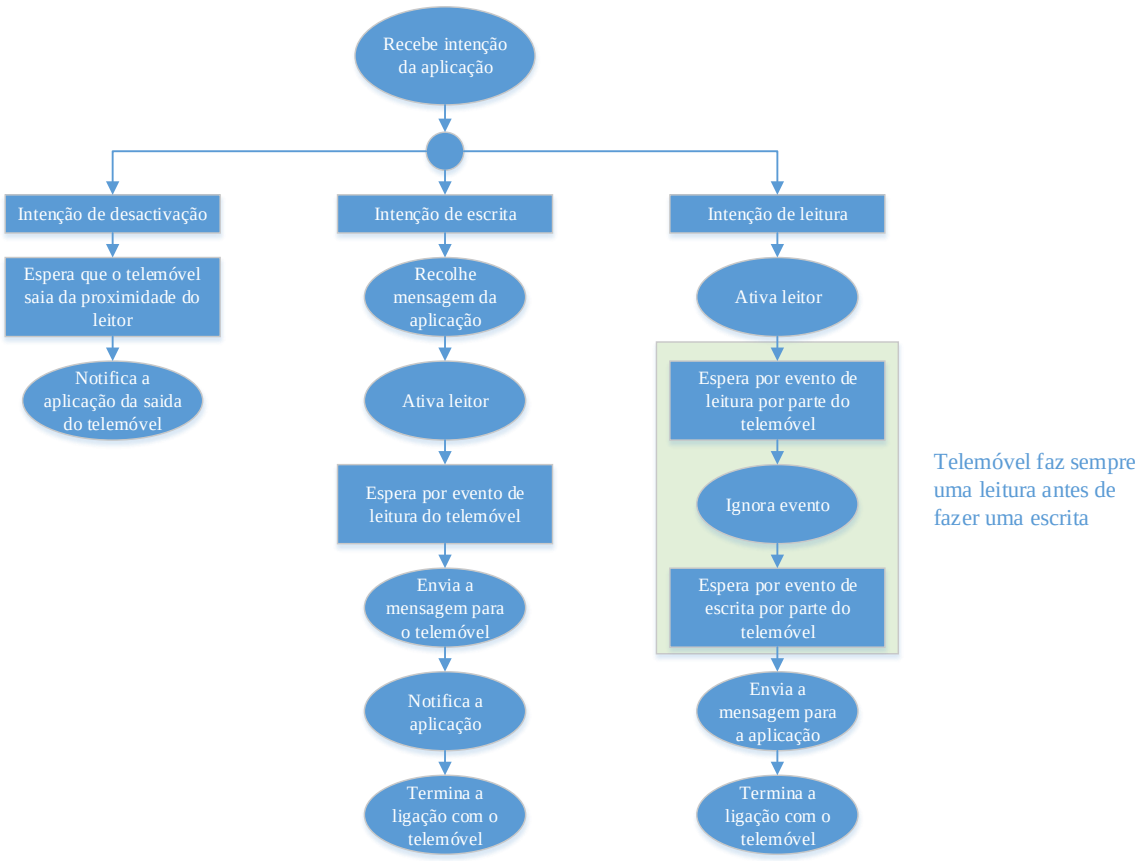


Figura 3.12 - Gestor de envio e receção de mensagens.

3.6.4. Identificação e validação do utilizador

A validação e identificação dos dados existentes no telemóvel requer o desenvolvimento de um protocolo de segurança para contornar possível cópia dos dados de um telemóvel para o outro. Visto não haver localmente no telemóvel um elemento seguro em hardware que garanta um ID único e não violável, e evitando uma ligação remota para autenticação, criou-se um protocolo de segurança localmente.

O protocolo de segurança é baseado na criação de chaves no momento da transação e o seu armazenamento no telemóvel e no servidor de autenticação. Quando existe nova transação a chave da transação anterior é validada e atualizada tanto no telemóvel como no servidor. Caso a chave da transação anterior não for válida é pedida uma password para identificar o utilizador. O protocolo de segurança está representado no diagrama da Figura 3.13.

Este protocolo de segurança foi desenvolvido para contornar a clonagem dos dados de um telemóvel para o outro, assim, cada vez que se dá uma transação as chaves são alteradas deixando os clones inválidos.

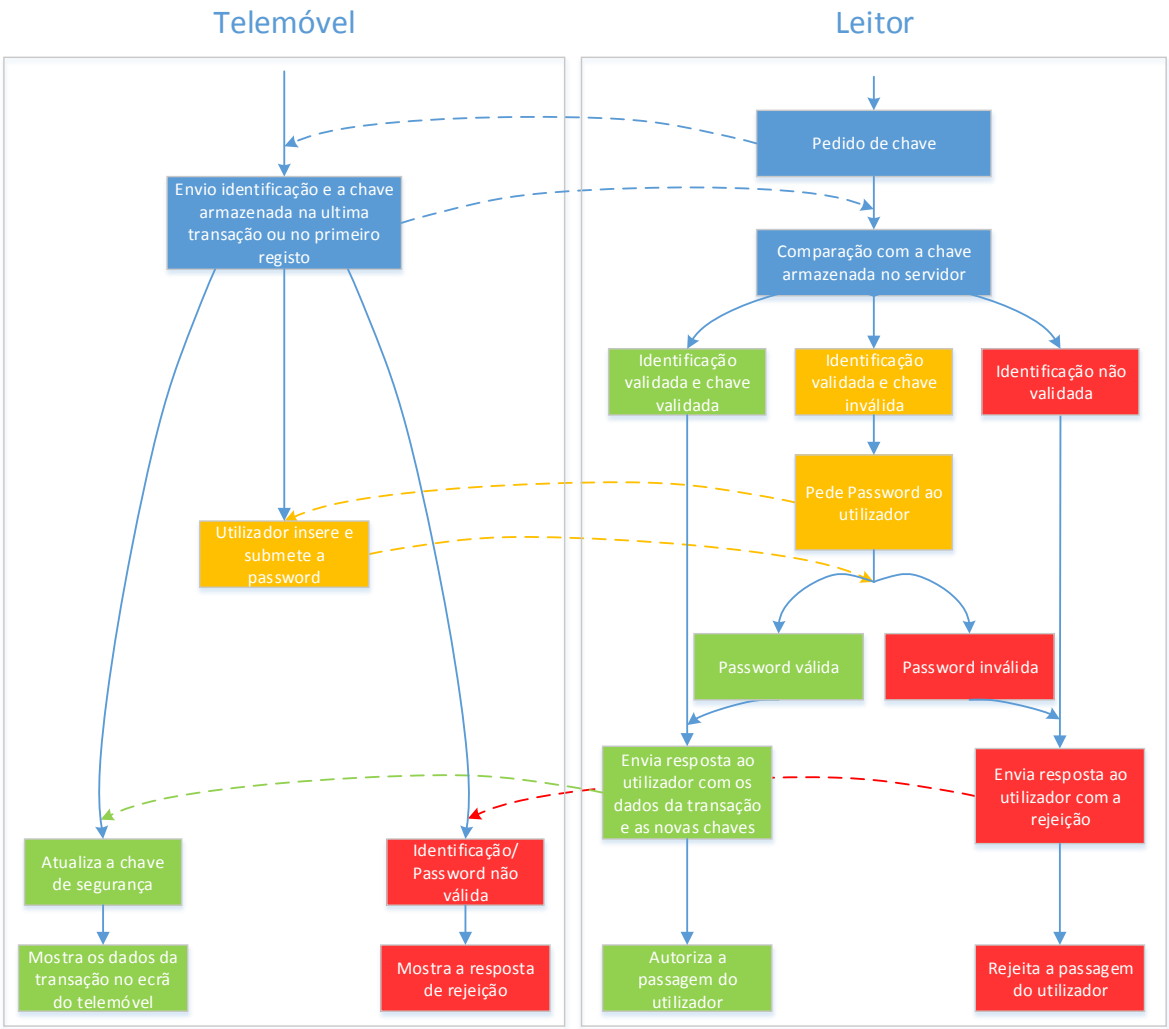


Figura 3.13- Protocolo de segurança desenvolvido.

3.7. Aplicação Android

A aplicação foi desenvolvida para ser compatível com dispositivos Android versão 4.3 ou superior. A aplicação está preparada para funcionar em qualquer versão do Android que suporte comunicação com *tags* do tipo 4. Para haver comunicação da aplicação com o leitor, é necessário que as comunicações NFC estejam ativas e o telemóvel no estado desbloqueado.

Um dos requisitos da aplicação era que esta fosse de rápido e fácil manuseio no ato de interagir com o leitor da portagem, assim a aplicação foi pensada para ser lançada automaticamente quando encostada ao leitor, sem que o utilizador tenha que intervir. O sistema operativo Android permite que as aplicações NFC sejam lançadas automaticamente quando for recebido um evento NFC específico. Para filtrar as mensagens especificas do leitor da portagem foi adicionado um *Intent Filter* ao ficheiro *AndroidManifest.xml* da aplicação que reencaminha a mensagem para aplicação quando a ação é do tipo NDEF_DISCOVERED e que contenha um *NDEF Record* do tipo *MIME-Type* com o tipo *"application/com.isel.portagensnfc"*. As seguintes linhas foram adicionadas ao ficheiro da aplicação android:

```
<intent-filter>
      <action android:name="android.nfc.action.NDEF_DISCOVERED" />
      <category android:name="android.intent.category.DEFAULT" />
      <data android:mimeType="application/com.isel.portagensnfc" />
</intent-filter>
```

Sempre que o leitor envia uma mensagem para o dispositivo móvel tem que incluir uma mensagem deste tipo para que esta seja corretamente reencaminhada para a aplicação pelo sistema operativo. Caso a aplicação se encontre fechada será aberta automaticamente.

3.7.1. Estrutura da aplicação

A aplicação está estruturada de acordo com o diagrama da Figura 3.14. O menu principal dá acesso a 3 menus, Conexão NFC, Log de passagens e os Gastos.

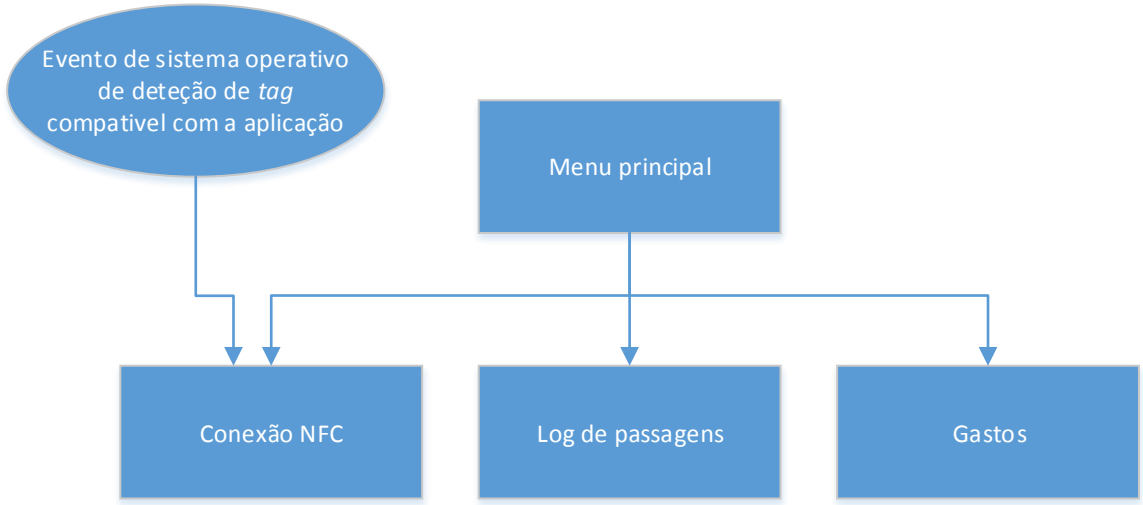


Figura 3.14 – Estrutura da aplicação.

Menu Conexão NFC

O menu da Conexão NFC pode ser aberto pelo utilizador através do menu principal ou automaticamente, sem a intervenção do utilizador, através de um estímulo externo do leitor. Este menu permite visualizar se o telemóvel está a comunicar com o leitor e o resultado da transação onde apresenta a informação do tipo de portagem, local de passagem, custos, data e hora.

Log de passagens

Neste menu são apresentadas todas as passagens em que o utilizador usou o telemóvel com NFC para efetuar a transação.

Gastos

Este menu permite ver os gastos mensais para um melhor controlo do utilizador na sua conta.

3.7.2. Fluxo da aplicação

Ao iniciar uma comunicação NFC com o leitor da portagem, a aplicação começa por validar o leitor, após validação envia as informações de identificação e receber a resposta positiva ou negativa por parte do leitor, de seguida informa o utilizador do resultado da transação. O fluxo está representado no diagrama da Figura 3.15.

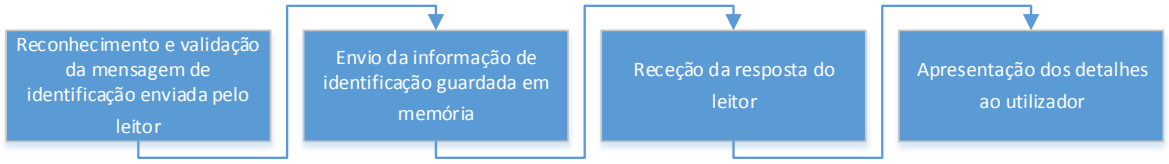


Figura 3.15 – Fluxo da aplicação.

4. Resultados

4.1. *Hardware* de desenvolvimento

Neste projeto foram usados dois dispositivos com tecnologia NFC para simular uma transação efetuada por um utilizador e para comparar resultados em termos de compatibilidade, de performance (tempos de transação) e distâncias de comunicação com o leitor. Do lado do leitor foi usado um kit de desenvolvimento com uma antena já integrada na PCB e o *transceiver* PN532 introduzido em 3.2.1 bem como uma plataforma de processamento para controlo do transceiver, o Raspberry Pi [22].

4.1.1. Smartphones

No desenvolvimento deste projeto foram usados dois dispositivos com tecnologia NFC e sistema operativo Android, um Nexus 7 [23] e um Samsung Galaxy S4 GT-I9515 [24], ambos com a versão 4.4.2 (Jelly Bean) [25] do Android.

Asus Nexus 7

O tablet Nexus 7 foi lançado em 2012 numa parceria da Asus e da Google, com a tecnologia NFC incluída. Contém um chip da NXP incorporado, o PN65, representado na Figura 4.1, que engloba um controlador PN544 [26] e um elemento seguro para efetuar transações seguras no sistema de pagamentos Google Wallet. Os componentes NFC vêm ativos por defeito em qualquer versão deste modelo, estando disponível para desenvolvimento e interação usando a API da Google [2]. A antena encontra-se localizada na estrutura de plástico do tablet na parte superior traseira do mesmo como se pode visualizar a azul na Figura 4.2.

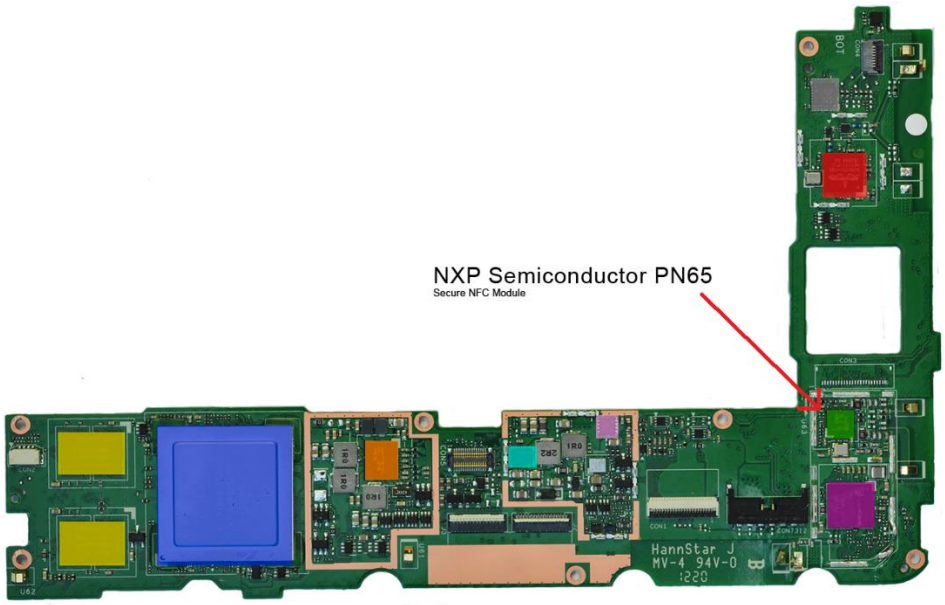


Figura 4.1 - Identificação do chip NFC na PCB do Nexus 7.

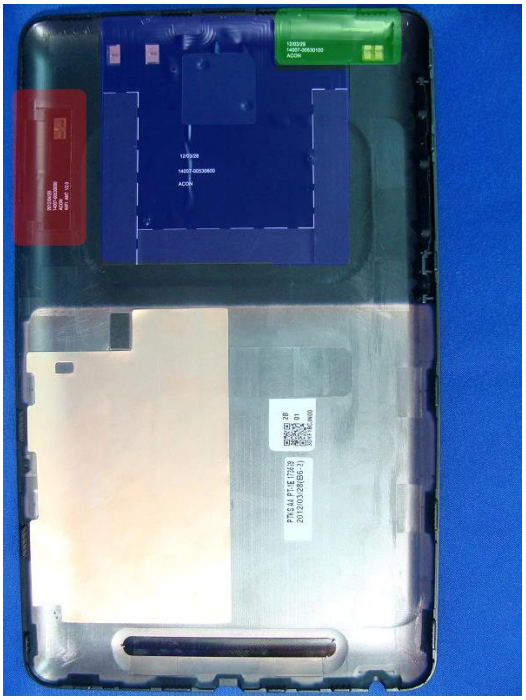


Figura 4.2 - Localização das antenas no Nexus 7

Samsung Galaxy S4

A Samsung lança o Samsung Galaxy S4 em Março de 2013 em que manteve o modelo e a estrutura dos componentes NFC, o transceiver continua a ser o PN544, representado com o numero 15 na Figura 4.4. O transceiver está conectado a uma antena em forma de loop que

está presente na parte exterior da bateria, ficando virada para a traseira do *Smartphone*, representação na Figura 4.3, sendo dois dos contactos da bateria reservados para o sinal RF da comunicação NFC.

Figura 4.3 - Posicionamento da antena no *Smartphone*.

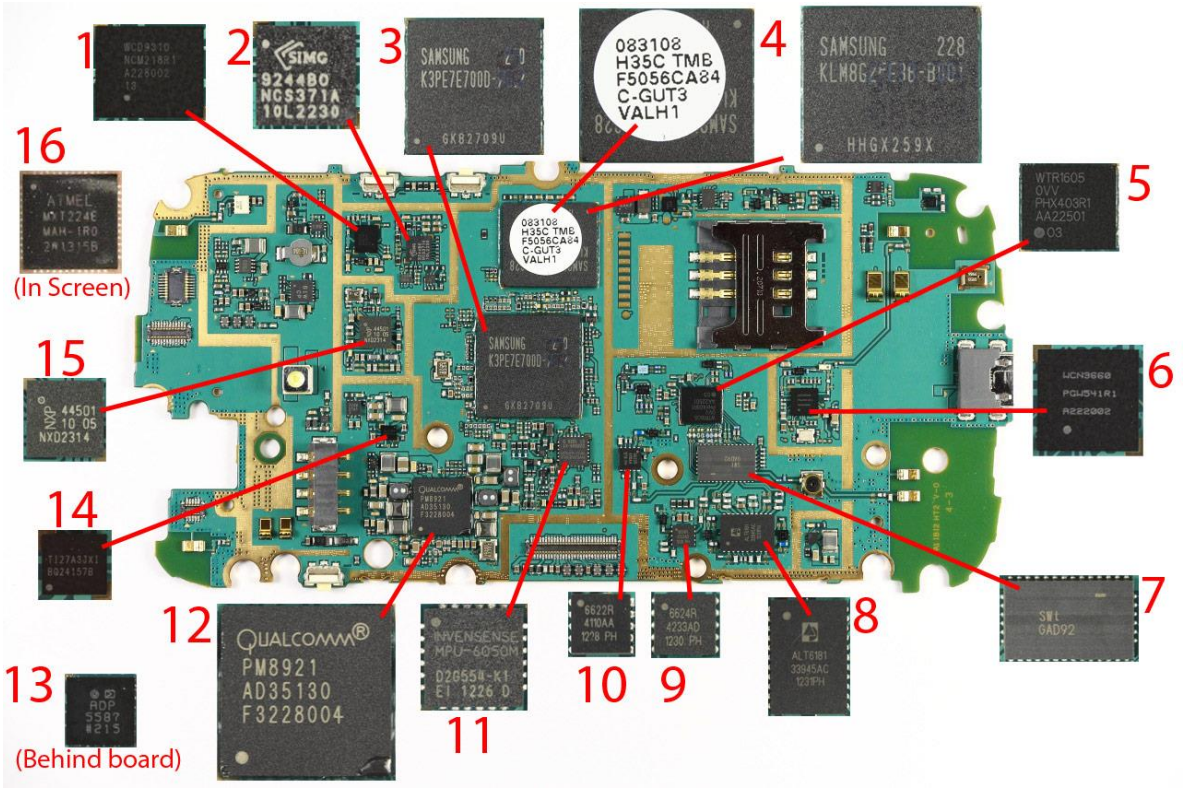


Figura 4.4 - Componentes de Hardware do Samsung Galaxy S4.

4.1.2. Raspberry Pi

A versão do Raspberry Pi utilizado para desenvolver este projeto de mestrado foi o modelo B que dispõe de um chip Broadcom BCM2835 que contém integrado um processador ARM1176JZF-S de 700MHz com 512MB de RAM e um processador gráfico VideoCore IV [27]. Como sistema operativo é usado o Raspbian [28] baseado na distribuição Debian [29] do Linux.

4.2. Leitor da portagem

Para implementar a comunicação NFC do lado da portagem foi usado uma placa de desenvolvimento que já contém o transceiver NFC PN532, a antena e a circuitaria necessária à sua operação, o esquemático encontra-se no Anexo 7.1. A placa de desenvolvimento é produzida pela Adafuit e está representada na Figura 4.5. A placa dispõe de pinos externos que disponibiliza a interface SPI para envio e receção de comandos, bem como os pinos de alimentação.

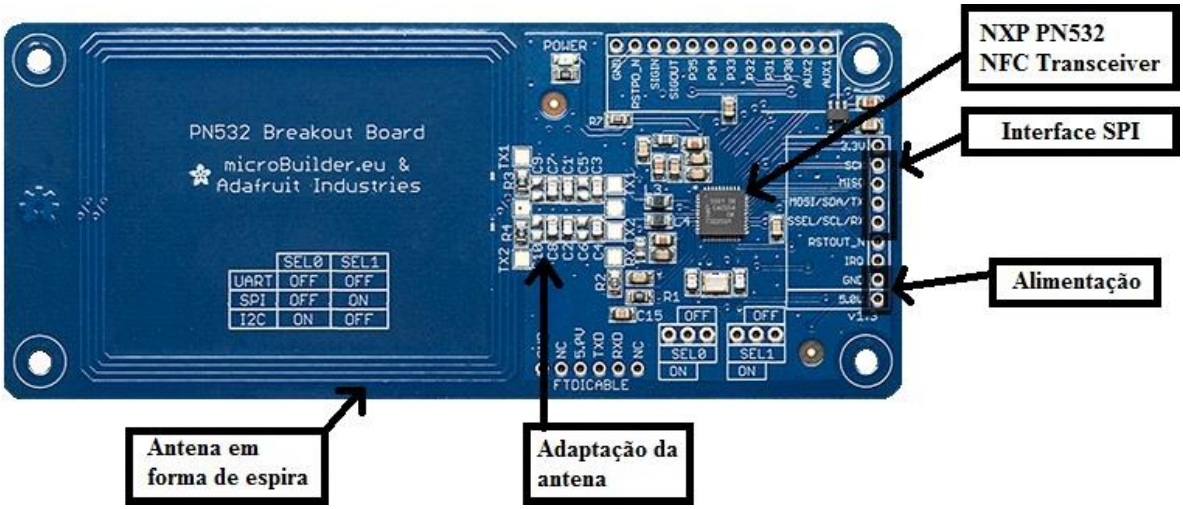


Figura 4.5 - Kit de NFC produzido pela Adafruit.

Para comunicar e alimentar a placa NFC foi desenvolvida uma PCB para interligar e fixar a placa ao Raspberry Pi, de forma a compactar todo o hardware necessário num só modulo para um fácil manuseamento e utilização. A Figura 4.6 mostra a placa desenvolvida, a azul, encaixada no Raspberry Pi, no Anexo 7.2 está disponível o esquemático e o desenho em .2D da placa.

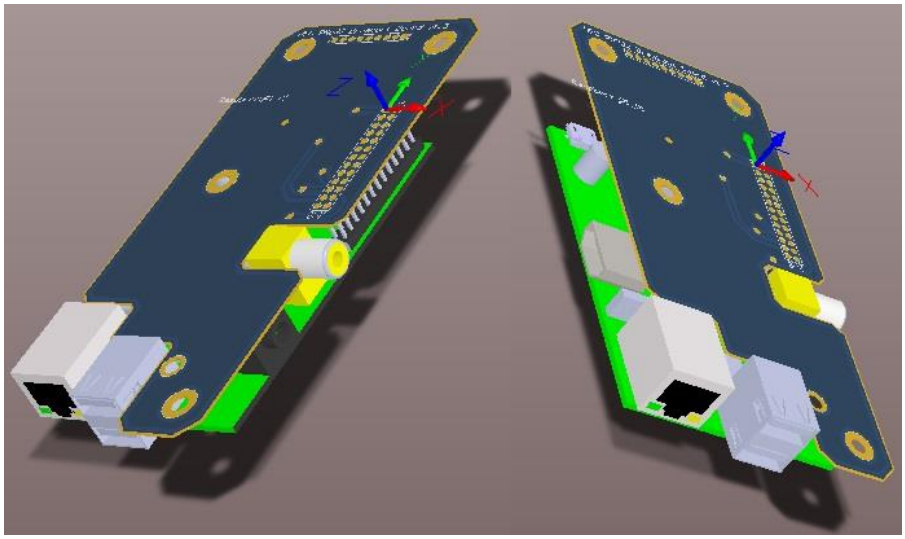


Figura 4.6 - Placa de adaptação Raspberry Pi / Placa NFC.

4.3. Aplicação Android

A aplicação foi desenvolvida para que fosse lançada automaticamente lançada assim que o telemóvel é encostado ao leitor NFC, dando inicio à transação e mostrando no final o ecrã com todos os detalhes. Na Figura 4.7 está representado o ecrã final de uma transação com um custo de 2.66€, a 26/09/2014 em Alverca.

Figura 4.7 - Menu da aplicação que mostra o resultado da transação efetuada.

4.4. Distâncias de comunicação

Para medição da distância máxima de comunicação foram colocados espaçadores entre o leitor da portagem e o *Smartphone* como é possível visualizar na Figura 4.8, após se verificar que não havia comunicação entre o leitor e o *Smartphone* os espaçadores foram encurtados em passos de $1mm$ até os dois conseguirem comunicar. Pela Figura 4.8 é possível medir a distância máxima à qual foi possível comunicar, $3.9cm$. O resultado para o tablet Nexus 7 foi igualmente $3.9cm$.

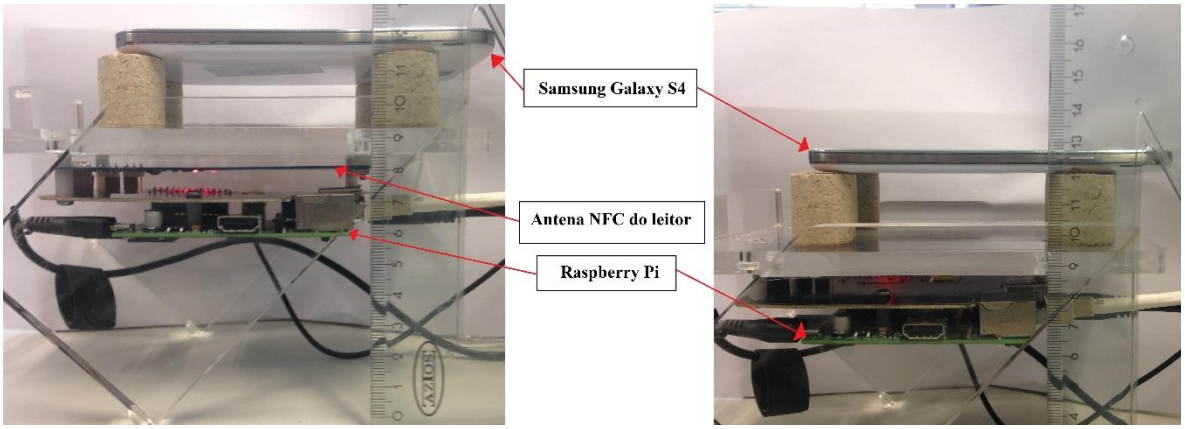


Figura 4.8 - Distância máxima de comunicação Samsung Galaxy S4.

4.5. Tempos de transação

Para medir os tempos de uma transação entre os dois dispositivos, recorreu-se a funções temporais disponibilizadas no Linux. Assim foi possível medir o tempo despendido nas 3 operações que constituem uma transação completa, estas estão representadas no diagrama temporal da Figura 4.9.

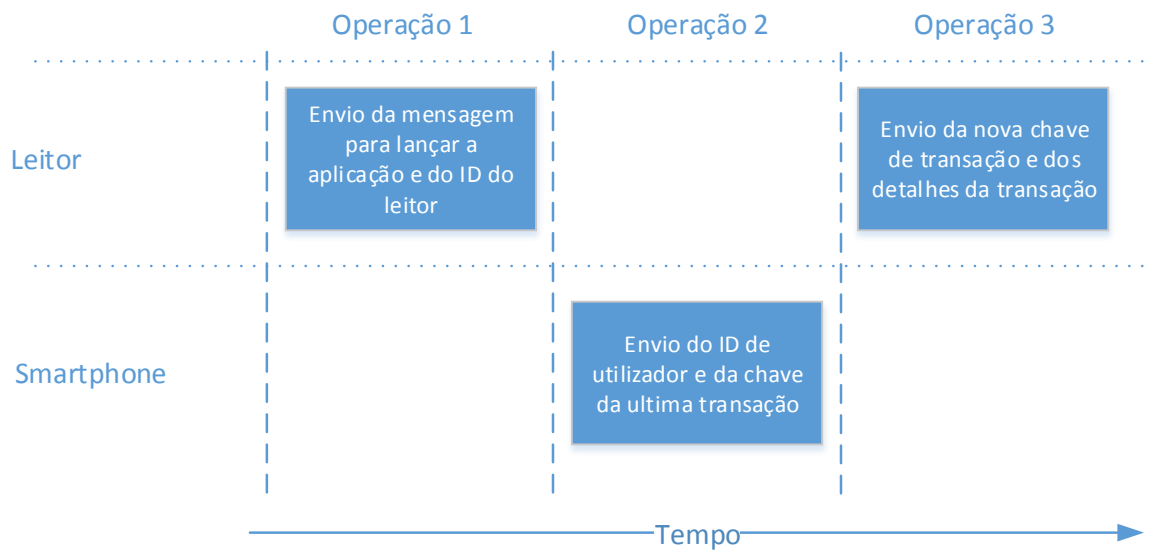


Figura 4.9 - Diagrama temporal da transação.

A primeira, a mensagem enviada pelo leitor que lança a aplicação do *Smartphone* e identifica o leitor, a segunda, a mensagem enviada pelo *Smartphone* com o seu identificador e a chave da última transação, a terceira, o envio da parte do leitor da nova chave e detalhes de transação. Nas figuras Figura 4.10, Figura 4.11 e Figura 4.12 estão representados os resultados dos tempos de cada operação para o Samsung Galaxy S4, para obter tempos fidedignos repetiu-se as operações 50 vezes.

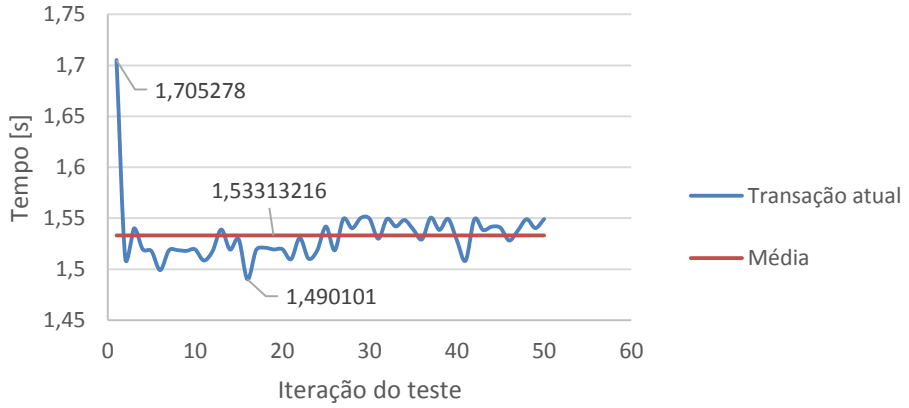


Figura 4.10 – Tempos da primeira operação para o Samsung Galaxy S4.

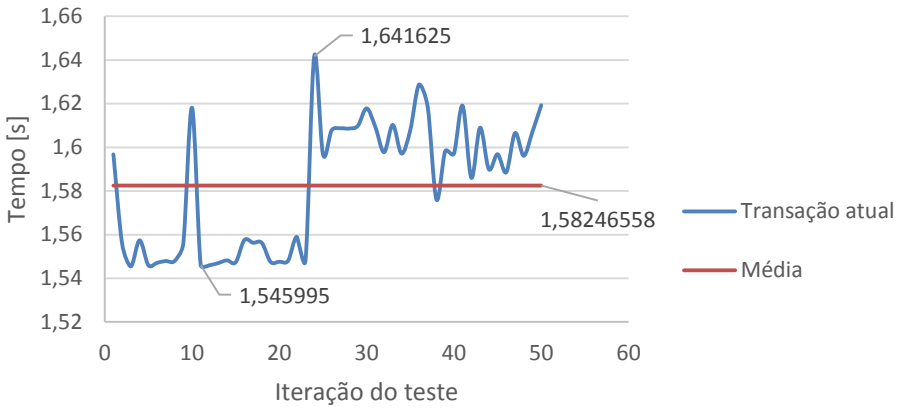


Figura 4.11 - Tempos da segunda operação para o Samsung Galaxy S4.

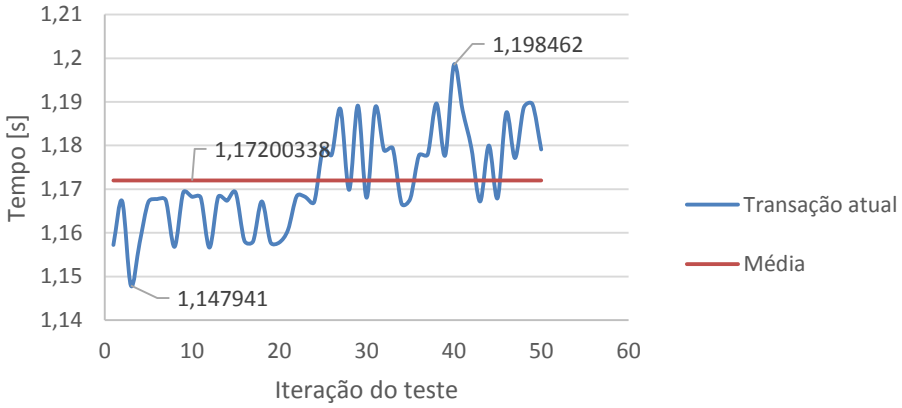


Figura 4.12 - Tempos da terceira operação para o Samsung Galaxy S4.

Foram igualmente retirados tempos para o dispositivo Asus Nexus 7, estão representados nas figuras Figura 4.13,Figura 4.14 e Figura 4.15.

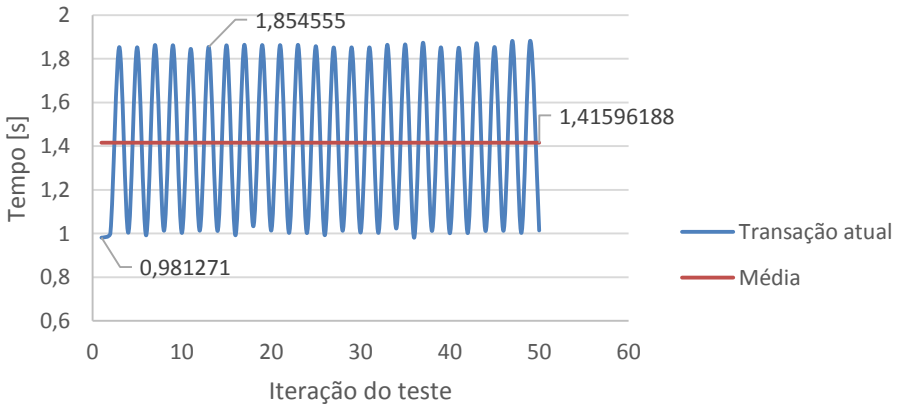


Figura 4.13 - Tempos da primeira operação para o Asus Nexus 7.

Figura 4.14 - Tempos da segunda operação para o Asus Nexus 7.

Figura 4.15 - Tempos da terceira operação para o Asus Nexus 7.

A

Tabela 4.1 mostra um resumo dos tempos de transação dos dois dispositivos testados. O tempo de uma transação completa demora aproximadamente 4.3 segundos em ambos os dispositivos. Na Operação 1 e 3 o *Smartphone* apenas necessita de fazer uma leitura, na Operação 2 é necessário fazer uma leitura e uma escrita, daí a operação 2 ser a mais demorada entre as 3. Nos gráficos das figuras Figura 4.16 e Figura 4.17 estão representados os tempos efetivos em que o leitor está a transferir os dados com o *Smartphone*. Numa operação de envio de dados para o *Smarthone* obtém-se um tempo médio de $564ms$ e numa operação de receção de dados do *Smartphone* um tempo médio de $968ms$. Não esquecendo que o envio de dados para o *Smartphone* apenas corresponde uma operação de leitura de *tag* por parte do

mesmo, enquanto que a receção de dados requer uma operação de leitura seguida de uma de escrita, o que explica a diferença de tempos.

Tabela 4.1 - Tempos de transação.

	Identificação do Leitor [s]			Envio do ID e da chave armazenada no *Smartphone* [s]			Envio da nova chave e detalhes da transação [s]			Tempo total despendido pelas funções de envio e receção [s]		
	Mín	**Méd**	**Máx**	**Mín**	**Méd**	**Máx**	**Mín**	**Méd**	**Máx**	**Mín**	**Méd**	**Máx**
Samsung Galaxy S4	1,148	1,533	1,705	1,546	1,582	1,642	1,148	1,172	1,198	3,842	4,288	4,545
Asus Nexus 7	0,981	1,416	1,855	1,565	1,580	1,608	1,286	1,297	1,324	3,831	4,293	4,786

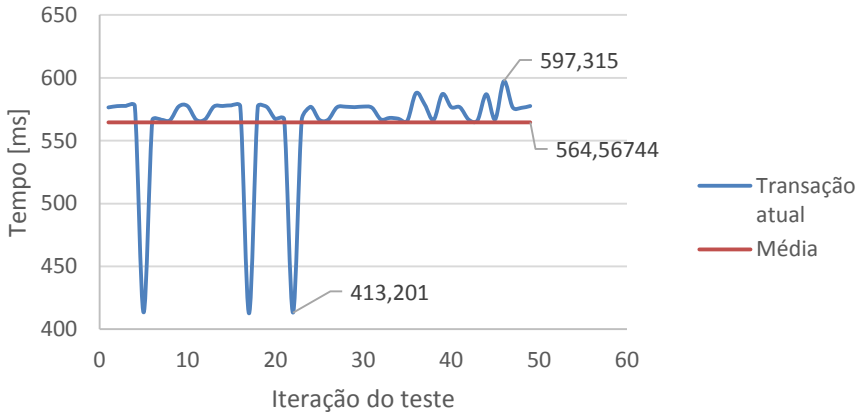


Figura 4.16 - Tempo efetivo de uma operação de envio de dados para o *Smartphone*

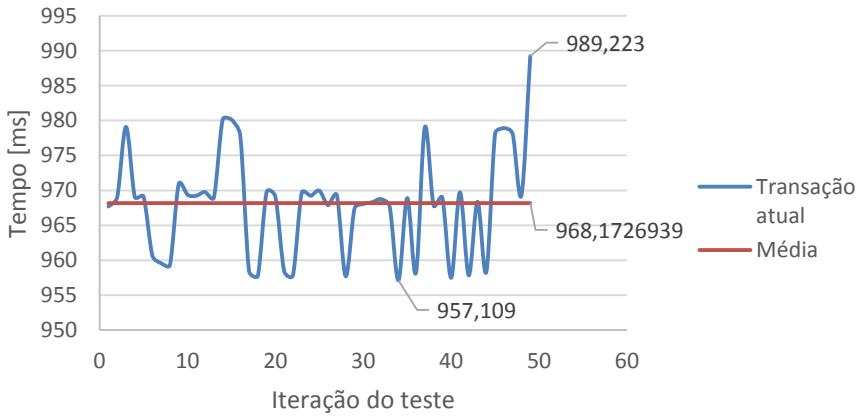


Figura 4.17 - Tempo efetivo de uma operação de receção de dados do *Smartphone*

Na Tabela 4.2 está feito um resumo dos tempos médios despendidos pelo sistema operativo Android para responder ao iniciar de uma operação disputada pelo leitor da portagem. É possível verificar que este tempo, $2.195s$, é mais de metade do tempo total de uma transação completa.

Tabela 4.2 - Tempos despendidos pelo sistema operativo

	Operação 1 [ms]	Operação 2 [ms]	Operação 3 [ms]	Total [ms]
Asus Nexus 7	447,787	1015,132	732,642	2195,562

4.6. Cenários de corrupção do sistema

O sistema de identificação tem dois cenários em que pode ser contornado por uma aplicação alterada mal-intencionada. Admitindo que o utilizador ou um individuo não autorizado tem acesso à memória onde estão armazenadas a identificação e chaves da aplicação, poderá copia-la e colocar noutro telemóvel fazendo-se passar pelo telemóvel que tinha o conteúdo original.

Cópia e uso dos dados sem autorização

Cenário em que a cópia é feita sem a autorização/conhecimento do proprietário e usada para se identificar em portagens fazendo-se passar por um utilizador válido. Neste caso o burlador terá um clone válido até a conta ser desativada ou até o proprietário usar de novo o telemóvel numa portagem. Caso o proprietário use o telemóvel numa portagem antes do burlador, o clone nunca chegará a ser válido, sendo pedida ao clone a password de conta quando apresentado na portagem.

Cópia e uso dos dados com autorização do proprietário

A cópia é feita com conhecimento do proprietário para outra pessoa usar a mesma conta para passar nas portagens. Neste caso quando o clone estiver com as chaves inválidas, a password será pedida, mas como é do conhecimento do utilizador do clone o telemóvel será validado.

Este tipo de clonagem propositada terá que ser detetada por constante validação do dispositivo através de password.

5. Conclusões

A tecnologia NFC presente nos telemóveis atualmente, existe como mais uma via de comunicação para com os mesmos, contrariando grande parte das comunicações sem fios onde se pretende grandes alcances, esta comunicação é feita quase com os dispositivos encostados sendo uma mais-valia para transações seguras de dados.

O desenvolvimento deste sistema teve como objetivo ser um sistema de pagamentos rápido, flexível e de fácil manuseio, em que o utilizador tivesse o mínimo de interação com o telemóvel e com a portagem, sendo apenas necessário encostar o telemóvel ao leitor para efetuar a transação e seguir viagem, objetivo que foi cumprido na totalidade.

O desenvolvimento deste projeto teve um maior foco nos protocolos e normas NFC que poderiam criar e oferecer uma ligação bidirecional para livre troca de dados ao nível da aplicação, o que não foi diretamente oferecido pelo sistema operativo Android, levando a uma mudança do rumo tomado a meio do projeto. Esta mudança fez com que se tivesse de deixar a especificação LLCP (peer-to-peer) oferecida pelo NFC-Forum, devido a limitações impostas pela API do Android, tendo de optar por emulação de uma *tag* de tipo 4 para criar a ligação bidirecional.

A aplicação do telemóvel foi desenvolvida para que fosse compatível com qualquer dispositivo com tecnologia NFC e sistema operativo Android, não tirando partido de nenhuma característica em particular dos dispositivos usados no projeto.

O protocolo utilizado neste projeto (emulação de *tag* de tipo 4) não está preparado para uma troca de dados bidirecional, pelo que o sistema operativo Android introduz um grande tempo de descoberta da *tag* cada vez que necessita de fazer uma escrita ou uma leitura na *tag*.

No que toca à segurança este projeto foi desenvolvido com o objetivo de o telemóvel não necessitar de uma ligação remota para efetuar a transação, mas o facto de os telemóveis não conterem elementos seguros para realizar uma autenticação local faz com que o nível de segurança seja limitado, sendo necessário outro tipo de abordagem. A existência de uma ligação remota a um servidor poderia permitir fazer uma autenticação em fonte segura, no entanto iria adicionar um tempo extra à transação.

5.1. Trabalho futuro

Como trabalho futuro passaria por estudar e abordar outras especificações da tecnologia NFC que permitissem uma maior flexibilidade na troca de dados bidirecional e que fosse compatível com o sistema operativo Android, em alternativa à emulação de *tag* do tipo 4 usada neste projeto.

No que toca à segurança, implementar a aplicação com recurso a uma ligação remota para proceder a uma autenticação numa fonte segura, avaliando o seu impacto no tempo da transação e na comodidade do utilizador.

Com o recente lançamento da versão 6 do iPhone com tecnologia NFC, passaria por analisar a que nível a tecnologia está disponível para desenvolver aplicações que interajam com o *transceiver* NFC disponível no telemóvel.

6. Bibliografia

[1] E. d. P. “Portugal Tolls,” 2012. [Online]. Available: http://www.portugaltolls.com/.

[2] Google, “Near Field Communication,” [Online]. Available: https://developer.android.com/guide/topics/connectivity/nfc/index.html.

[3] “Via Verde,” [Online]. Available: http://www.viaverde.pt/Website/.

[4] “NFC Forum,” 2004. [Online]. Available: http://nfc-forum.org/.

[5] ISO/IEC, “ISO/IEC 18092:2013, Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1),” ISO/IEC, 15 03 2013. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56692. [Acedido em 28 01 2014].

[6] M. Roberti, “The History of RFID Technology,” RFID Journal, 16 01 2005. [Online]. Available: http://www.rfidjournal.com/articles/view?1338. [Acedido em 28 01 2014].

[7] P. Preuss, “NFC Use Cases,” NFC Forum, 9 2009. [Online]. Available: http://members.nfc-forum.org/events/oulu_spotlight/Forum_and_Use_Cases.pdf. [Acedido em 1 2 2014].

[8] M. Kerschberger, “Near Field Communication, A survey of safety and security measures,” 17 07 2011. [Online]. Available: https://www.auto.tuwien.ac.at/bib/pdf_TR/TR0156.pdf. [Acedido em 5 2 2014].

[9] N. F. “NFC Forum Technical Specifications,” NFC Forum, [Online]. Available: http://members.nfc-forum.org/specs/spec_list/. [Acedido em 12 03 2014].

[10] Google, “Google Wallet,” 2014. [Online]. Available: https://www.google.com/wallet/. [Acedido em 2014].

[11] H. S. Kortvedt, “Master Tesis in Science in Communication Technology, Securing Near Field Communication,” 2009.

[12] Z. Kfir e A. Wool, “Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems,” 22 02 2005. [Online].

[13] F. D. Garcia, G. d. K. Gans, R. Muijrers, P. v. Rossum, R. Verdult, R. W. Schreur e B. Jacobs, “Dismantling MIFARE Classic,” Institute for Computing and Information Sciences, Radboud University Nijmegen. [Online].

[14] “FeliCa - Contactless IC Card Technology,” Sony, [Online]. Available: http://www.sony.net/Products/felica/business/products/RC-S860.html. [Acedido em 06 05 2014].

[15] N. F. “NFC Logical Link Control Protocol (LLCP) Technical Specification,” [Online]. [Acedido em 1 Agosto 2014].

[16] “ISO/IEC 18092:2013,” [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=56692. [Acedido em 5 Agosto 2014].

[17] nfc-tools, “Libllcp,” [Online]. Available: http://nfc-tools.org/index.php?title=Libllcp. [Acedido em 3 Junho 2014].

[18] Google, “Android Beam,” [Online]. Available: http://developer.android.com/guide/topics/connectivity/nfc/nfc.html#p2p. [Acedido em 25 Maio 2014].

[19] N. F. “NFC Forum Type 4 Tag Operation Specification 2.0,” 2011.

[20] ISO/IEC, “ISO/IEC 7816-4, Identification cards — Integrated circuit - Part 4: Organization, security and commands for interchange,” 2005.

[21] N. S. N. “MIFARE DESFire EV1,” 2012.

[22] R. P. Foundation, “Raspberry Pi,” [Online]. Available: http://www.raspberrypi.org/.

[23] Asus, “Nexus 7,” [Online]. Available: http://www.asus.com/pt/Tablets/Nexus_7/.

[24] Samsung, “Galaxy S4,” [Online]. Available: http://www.samsung.com/pt/consumer/mobile-phone/smartphones/android/GT-I9505ZWATPH.

[25] Google, “Android 4.2 APIs,” [Online]. Available: http://developer.android.com/about/versions/android-4.2.html.

[26] NXP, NFC controller PN544 for mobile phones and portable equipment, NXP, 2010.

[27] Wikipédia, “Raspberry Pi,” [Online]. Available: http://en.wikipedia.org/wiki/Raspberry_Pi.

[28] Raspbian. [Online]. Available: http://www.raspbian.org/.

[29] Debian. [Online]. Available: https://www.debian.org/index.pt.html.

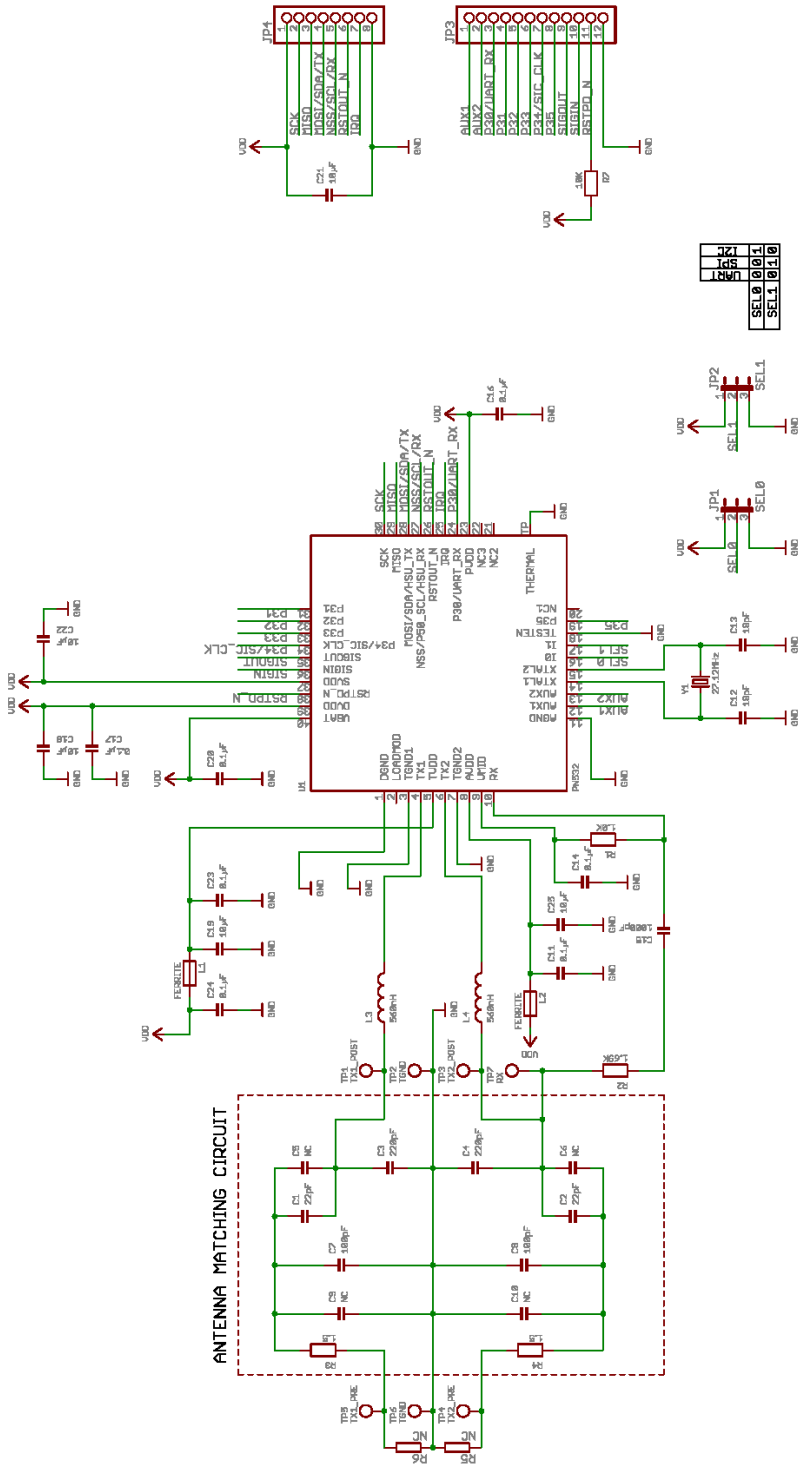
[30] N. F. “NFC Data Exchange Format (NDEF) Technical Specification,” [Online]. [Acedido em 2 Agosto 2014].

[31] Google, “Android 4.4 APIs,” [Online]. Available: http://developer.android.com/about/versions/android-4.4.html.

[32] Samsung, “Galaxy S III,” [Online]. Available: http://www.samsung.com/pt/consumer/mobile-phone/smartphones/android/GT-I9300MBDTPH.

7.Anexos

7.1. Esquemático da PCB do transceiver NFC presente na portagem



7.2. PCB de adaptação Raspberry Pi / Placa NFC