The use of SmartCard authentication as a medium for protecting Taxi passengers

Cesar Augusto Bonilla Alvarez

Technical Report
4 March 2015

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom
The use of SmartCard authentication as a medium for protecting Taxi passengers

Supervisor: Professor Keith Mayes

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date: August 29, 2014
ACKNOWLEDGEMENTS

At the outset I wish to acknowledge my gratitude to my family Carmenza, Victor and John Jairo for their tireless support during my studies.

I would also like to express my thanks to William, Mireya and their children.

Finally, I should like to thank all my fellow members very sincerely for their advice.
CONTENTS

1. Introduction ......................................................... 12
   1.1 Motivation .................................................. 13
   1.2 Goals ...................................................... 14
   1.3 Structure of the Project .................................. 14

2. Background ......................................................... 16
   2.1 Importance of the Taxi Industry ......................... 16
   2.2 Risks to passengers’ safety at the Taxi service ........ 18
   2.3 The taxicab secure booking applications ................. 21
   2.4 Types of (de)regulated taxicab industries .............. 22
   2.5 Summary .................................................. 25

3. Technical Background ............................................ 26
   3.1 Authentication ............................................. 26
      3.1.1 Unilateral dynamic symmetric authentication ...... 27
      3.1.2 Unilateral static asymmetric authentication ...... 27
      3.1.3 Unilateral dynamic asymmetric authentication ...... 30
   3.2 Elliptic curve cryptography ................................ 31
      3.2.1 Elliptic Curve Diffie-Hellman protocol (ECDH) ... 33
      3.2.2 The Elliptic Curve Digital Signature Algorithm (ECDSA) 35
   3.3 Near Field Communication .................................. 37
      3.3.1 Operation modes ....................................... 37
      3.3.2 NFC Data Exchange Format (NDEF) .................. 39
      3.3.3 NFC Tag types ....................................... 40
   3.4 Summary .................................................. 41

4. The TAXI Authentication scheme ................................. 42
   4.1 Security requirements for the taxicab authentication .... 42
      4.1.1 User safety .......................................... 42
      4.1.2 Quality service ....................................... 43
      4.1.3 System’s capabilities and efficiency ............... 43
   4.2 the TAXI System Architecture .............................. 44
      4.2.1 The Key Management System .......................... 47
4.2.2 The Station-to-station protocol ............................................. 50
4.3 Components ........................................................................... 53
  4.3.1 The TAXI Local Authority subsystem ................................. 53
  4.3.2 The TAXI Licence Operator subsystem ............................. 54
  4.3.3 The TAXI Mobile application ........................................... 55
  4.3.4 The TAXI Fare application ............................................... 56
4.4 Summary .................................................................................. 57

5. The Back-office processes .......................................................... 58
  5.1 Process 1. Administration of the Licence Operators ............... 58
    5.1.1 Process 1a. Licence Operator enrolment ......................... 58
    5.1.2 Process 1b. Licence Operator revocation ....................... 64
    5.1.3 Process 1c. Renovation of a Licence Operator ............... 65
  5.2 Process 2. Administration of taxicab licences ..................... 66
    5.2.1 Process 2a. Taxicab enrolment ....................................... 66
    5.2.2 Process 2b. Taxicab licence revocation ....................... 70
  5.3 Process 3. Up-to-date taxicab licences ................................. 71
    5.3.1 Process 3a. Taxicab enrolment ....................................... 71
    5.3.2 Process 3b. Taxicab licence revocation ....................... 71
  5.4 Process 7. Quality service statistics ..................................... 73
  5.5 Summary .................................................................................. 73

6. The Front-office processes .......................................................... 75
  6.1 Process 4. Control of users .................................................. 75
    6.1.1 Process 4a. User enrolment ........................................... 75
    6.1.2 Process 4b. Up-to-date licences ..................................... 78
  6.2 Process 5. the TAXI Authentication protocol ....................... 79
    6.2.1 Process 5a. Offline authentication mechanism ................ 79
    6.2.2 Process 5b. The Authentication event ............................. 83
  6.3 Process 6. The Quality service evaluation ............................ 86
  6.4 Summary .................................................................................. 89

7. Security Analysis ....................................................................... 90
  7.1 Analysis of the system requirements ..................................... 90
    7.1.1 User safety ................................................................. 90
    7.1.2 Quality service ............................................................ 93
    7.1.3 System’s capabilities and efficiency ............................. 94
  7.2 Analysis of real-world crimes ............................................... 95
    7.2.1 Kidnap a customer ’express kidnapping’ and lure crimi- 97
    nals into a taxi for robbery or sexual assault ......................
    7.2.2 Operate an illegal taxicab ’outing’ ................................. 100
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2.3 Undermine the quality service of the scheme</td>
<td>100</td>
</tr>
<tr>
<td>7.2.4 Falling to report incomes</td>
<td>101</td>
</tr>
<tr>
<td>7.3 Summary</td>
<td>101</td>
</tr>
<tr>
<td>8. Conclusions</td>
<td>102</td>
</tr>
<tr>
<td>8.1 Further work</td>
<td>103</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

2.1 The main role of the taxicab as a connector between night places and their customers: A taxi at Times Square in Midtown Manhattan, New York City [1]. ........................................... 18
2.2 Several models of taxicabs in an open-regulated scheme [2] .... 19
2.3 An advertisement of 'The Safer Travel at Night’ campaign [2] .... 22

3.1 Scheme of the authentication of a SIM card in a GSM Network [3] ......................................................... 28
3.2 An EMV contactless card [4] ................................................... 29
3.3 Comparison extracted from [5] about the performance between 1024-bit RSA and 160-bit ECDSA Digital signatures. *The 1024-bit RSA and 160-bit ECDSA schemes provide a near-equivalent level of security according to the figure 3.4* .... 31
3.4 Comparison of the level of security according the key length and cryptographic algorithm [6] ................................. 32
3.5 The Elliptic Curve Diffie-Hellman protocol (ECDH) ............. 34
3.6 An NFC mobile phone in card emulation mode[7] ............... 38
3.7 Structure of an NDEF message[8] ........................................ 39

4.1 the TAXI Authentication scheme ........................................ 45
4.2 Hierarchy of Digital Signature keys ..................................... 48
4.3 Cryptoperiod of the keys of the scheme beginning in 2015 .... 49
4.4 The Station-to-station protocol .......................................... 51
4.5 The TAXI Local Authority subsystem ................................. 53
4.6 The TAXI Licence Operator subsystem ............................... 55
4.7 The TAXI Mobile application ........................................... 56
4.8 The TAXI Fare application ................................................ 57

5.1 Process 1a. Licence Operator enrolment .............................. 60
5.2 Process 1b. Licence Operator revocation ............................. 64
5.3 Relation of lifetimes of Licence Operators and taxicab licences revocation ................................................... 66
5.4 Process 2a. Taxicab enrolment ................................. 67
5.5 Process 2b. Taxicab licence revocation .............................. 70
5.6 Process 3a. Taxicab enrolment ................................. 72
6.1 Process 4a. User enrolment ................................. 76
6.2 Process 4b. Up-to-date licences ............................... 78
6.3 Process 5a. The TAXI Authentication protocol .......... 84
6.4 Process 5b. The Authentication event ....................... 85
6.5 Process 6. The Quality service evaluation ............... 87
7.1 Analysis of the user safety requirements .................... 90
7.2 Analysis of the quality service requirements ............... 93
7.3 Analysis of System’s capabilities and efficiency requirements .... 94
7.4 Requirements Vs Processes ................................. 96
7.5 Diagram of a relay attack .................................. 99
7.6 Statistics of overlapped journeys of the same taxicab licence number ................................................. 100
ACRONYMS

ABI The Association of British Investigators
AES Advanced Encryption Standard
ANSI American National Standards Institute
APDU-C Application Protocol Data Unit Command
APDU-R Application Protocol Data Unit Response
AuC Authentication Centre
CA Certification Authority
CAM Card Authentication Mechanism
CBC Cipher Block Chaining
CDA Combined Data Authentication
CRL Certificate Revocation List
DDA Dynamic Data Authentication
DLP Discrete logarithm problem
ECDH Elliptic Curve Diffie-Hellman key agreement protocol
ECDLP Elliptic Curve Discrete Logarithm problem
ECDSA Elliptic Curve Digital Signature Algorithm
EMV Europay Mastercard Visa
FIPS Federal Information Processing Standards
GBP Pound sterling
GPS Global Positioning System
GSM  Global System for Mobile Communications
ICC  Integrated Circuit Card
IEC  International Electrotechnical Commission
IEEE  Institute of Electrical and Electronics Engineers
IMSI  International Mobile Subscriber Identity
ISO  International Organization for Standardization
JIS  Japanese Industrial Standards
KMS  Key Management System
LCC  London Chamber of Commerce
LTE  Long-Term Evolution Network
MAN  Metropolitan Area Network
MNO  Mobile Network Operator
NDEF  NFC Data Exchange Format
NFC  Near Field Communication
NFCIP-1  NFC Interface and Protocol
NFS  Number Field Sieve
NIST  National Institute of Standards and Technology
OS  Operating System
OTA  Over-The-Air technology
PDA  Personal Digital Assistant
PHV  Private Hire Vehicle
RSA  Rivest, Shamir and Adleman algorithm
RTD  Record Type Definition
SCMS  Smart Card Management System
SD  Secure Digital
List of Figures

SDA Static Data Authentication
SIM Subscriber Identity Module
SMS Short Messages Service
TFL Transport For London
TLS/SSL Transport Layer Security/Secure Sockets Layer
TPM Trusted Platform Module
UK United Kingdom
URL Uniform Resource Locator
UTF Unicode Transformation Format
VDS Vehicle Description Section
VHBR Very High Bit Rates
VIN Vehicle Identifier Number
VIS Vehicle Identifier Section
WiMAX Worldwide Interoperability for Microwave Access Network
WMI World Manufacturer Identifier
EXECUTIVE SUMMARY

The taxicab service industry has undergone a lot of change and some of them have decreased the safe of taxicab passengers. The document presents a description of major implications in three sectors of the economy. A brief explanation of some factors that affect directly the taxicab industry is given and how those become a threat for the perception of safety for the passengers. The document also presents three factors: the lack of provision of taxicabs leading to an increase of illegal taxicab market 'outing'; relaxation of requirements for taxicab drivers to get a licence and the adoption of a more deregulate scheme leading to a decrease in the level of passengers’ safety.

As a result, the TAXI authentication scheme is proposed to provide a fast mechanism for users to authenticate taxicabs in the street. At the root of the scheme is placed a Key Management System using ECDSA digital signatures whose public certificates are stored on the smart cards located on the taxicabs and users can execute an off-line asymmetric authentication protocol using their NFC-enabled devices as a reader.

The TAXI scheme is based on 14 requirements grouped in three categories: the user’s safety which intends the users hire a taxicab with a valid licence; quality service aiming to users to assess the quality of the service provided by the taxicab ensuring their privacy and assures the scheme can operate efficiently regardless the number of taxicabs or users have joined the system.

The scheme has four components: the TAXI Local Authority subsystem, the TAXI Licence operator subsystem, the TAXI Mobile application and the TAXI Fare application that meet the proposed requirements by means of seven processes which coordinate the procedures of issuing and revocation of both taxicab and Licence Operators licences, authentication of taxicabs, and evaluation of the quality service.

At the end, it is presented the security analysis of the scheme. First it starts with the processes of the TAXI scheme that address every proposed requirement. Second, how three different threats could undermine the system based on the factors presented on the beginning of the document. Finally, which controls mitigate the threats.
1. INTRODUCTION

The public passenger transport is considered an essential public service in the majority of metropolitan cities around the world. However, in most of them only the taxicab service is available 24 hours a day, 365 days a year. Despite this, it is sometimes not seen as a public service due to its nature, which a user obtains a more personalised service by the transport operator highly dependent on the trustworthiness between the driver and her or his passenger [9]. Moreover, when there is an increasing trend towards enhancing competition in order to decrease taxicab fares by means of an increase in the number of operators yielding the increased risk for crime in the taxicab service [10, 11, 12].

All sectors of the modern society have been affected by any criminal, means of transport are not excluded from this phenomenon. The Taxi service is one of the vital services in modern cities. It offers a reliable and safe mode of transportation when other means of transportation are not available or less suitable for the needs of customers. However, there has been recently an increase of disturbing incidents involving taxis around the world, with passengers suffering from incidents such as sexual assaults, armed robbery or express kidnappings [13, 14, 15, 16]. Despite of the fact that users usually boost their perception of security when hail a taxi in the street using different methods described by Kaiser [17], the need for authentication of taxicabs is evident because current taxicab booking applications do not provide sufficient functionality, usability or convenience for taxi users and then, their use is scarcely adopted by the general public [18, 19].

The process of authentication is traditionally done by three methods [20]:

- something you know
- something you are\(^1\)
- something you have

\(^1\) There is another method called "Something you do". It sometimes associated with the field of biometrics: when a user is authenticated by the way he or she types on a keyboard (keystroke dynamics), writes a signature, or simply by pushing a button on a wireless device (SecureEasySetup)\(^{20}\)
The method called “Something you know” is the most recognised authentication method although it is susceptible from a great number of attacks becoming the most vulnerable method of authentication. Passwords belong to this category and they are vulnerable to several attacks such as replay, dictionary and brute force attacks among others. The second, “something you are” is only valid for authenticating human beings, biometrics is a field which studies physical characteristics on humans in order to make possible to identify and authenticate them simultaneously. The last method, “something you have”, is characterised by the use of tokens. They serve to identify and authenticate both people and entities. The Smart Cards are between the most advance tokens trading off security and flexibility. The use of cryptographic functions and tamper-resistant mechanisms placed on them make an ideal technology for authentication entities such as taxicabs.

Another technology increasingly accepted by the general market is the Near Field Communication technology (NFC). The technology provides a reliable channel by using electromagnetic radio waves for short-range communication, with the option of establishing a secure channel. Furthermore, it is fully supported by international standards, making it highly interoperable, ideal for great diverse of applications. Since its creation in 2002 has continued to expand in both mobile devices market, over 200 million NFC-enabled mobile phones deployed [21], and the application market, ranging from transportation ticketing [22, 23], access control and loyalty programs [24] to the most renowned NFC applications in the e-payment industry are Google wallet [25], Visa paywavemobile [26] and MasterCard paypass [27]. This is due to the fact that the NFC technology provides several key features such as the capability of an interaction with contactless smart cards, the ease to use for users to execute a function with a simple touch [28] and different modes of operation which convert the NFC-enabled device in a portable card reader or a Smart Card depending upon the application [29].

1.1 Motivation

According to a study conducted by TFL in 2009, more than half of customers hire a taxi in the street whereas one third of them engages a taxi at a rank and the number of customers who pre-book a taxi is negligible [30]. The figures show that hailing a taxi in the street is the most common way for a user to engage a taxi, which is just “ply for hire” [31]. Similar patterns of behaviour towards engage a taxi in the street are documented in other places around the world [32]. Moreover, taxi drivers prefer to pick users up in the street because it can take a long time to collect users who pre-book the service [33]. However, far too little attention has been paid to finding a solution to
authenticate taxis when they are hired in the street. This dissertation will present a novel authentication system which customers can check the identity of a taxi when hailing it in the street using NFC-capable devices.

1.2 Goals

The most important goal is to propose the TAXI scheme, acronym for *Taxi Authentication eXecuted by an Id-card scheme*, a new authentication scheme for the taxi industry that makes use of the NFC technology. In order to achieve the primary goal, three objectives were set:

- To define the requirements for the solution based on the issues which adversely affect the perception of personal safety for the taxicab passengers.
- To design a scheme which allow users to authenticate taxicabs in the street. The scheme should be capable of fulfilling the defined requirements by means of a system architecture, its major components and the critical processes for its proper functioning.
- To conduct an analysis of the security requirements of the described processes in order to corroborate the scheme satisfies the aims of the project and analyse to what extent the proposed solution will mitigate the problems jeopardising the taxicab passengers’ safety.

1.3 Structure of the Project

The second chapter presents a summary of the key points found on the literature review which exposes the reasons of the need to build an authentication system for the Taxicab industry in order to protect the perception of safety of taxi passengers.

The third chapter provides a brief overview of the technical concepts of entity authentication methods using on the Smart Cards; Elliptic curve cryptography and the NFC technology characteristics and its modes of operation.

The fourth chapter describes the TAXI Authentication scheme: the proposed security requirements for the project, the system architecture and its major components.

The Back-office processes are outlined in the fifth chapter: Administration of Licence Operators, taxicab licences and quality service statistics.

In the sixth chapter is explained the TAXI Authentication protocol using the NFC technology and contactless smart card and other Front-office processes of the scheme.
1. Introduction

The seventh chapter explains the Security Analysis and demonstrates in which extent the proposed protocol fulfils the security requirements and examines the mechanisms of the processes described in the previous chapter mitigate threats posed to the industry.

The eighth chapter concludes the document with a brief review of the key points of the solution and future developments.
2. BACKGROUND

This chapter highlights the importance of ensuring that taxicab users perceive the taxi service as safe. Although the issues affecting the taxicab passengers remains low [34], it is with regard to the number of taxicab journeys [35], developing a bad reputation could lead to negative consequences not only in the taxicab industry, but also in other sectors of the economy presented in the section 2.1. To illustrate that, the city of London has been selected to make clear those facts.

The section 2.2 describes different threats to the security in taxicabs which might cause an increase of the crimes against taxicab passengers such as sexual assaults [13], armed robbery and express kidnappings [15, 16, 36] or the issues that discourage users to use the taxi service such as bad quality service, disproportional taxi fares and lack of availability [35, 10, 11].

The section 2.3 enumerates a range of applications that intent to provide security for passengers. Finally, the section 2.4 describes the schemes which taxi industry is organised around the world.

2.1 Importance of the Taxi Industry

Taxicabs are the most important means of non-mass transportation: They supply a transportation service others cannot or will not do. Sometimes this is because the lack of sufficient market demand from the passengers, for example, during off-peak hours or in remote locations where a transportation network is not feasible. A further reason is comfort: Wheelchair users find it more convenient to use taxis as a substitute for public transport services. Travellers also find it easier to carry heavy luggage from/to airports or train or coach stations using taxi service [34]. The main economy sectors in which taxis are considered essential are the Business Environment, the Night-life sector and the Airport Industry.

The Business sector is one part of the economy in which the Taxicab Service plays an important role. Despite of the fact that most business managers have their own car, they prefer to use a taxi service when travelling to and from other places in order to attend a business meeting or engage in another kind of business activity. In a study made by the London Chamber of
Commerce (LCC) in 2007 about the perception of the taxi service by business directors in London, almost all highlighted the importance of having a reliable taxi service in the city. For example, retail service managers observed users using the service frequently while going shopping [34]. Directors of other sectors of the economy also emphasised the value of taxis on their respective sectors. Moreover, when they were consulted about the use of taxis in their daily life, they often responded that they used the taxicab service to travel to business meetings and nearly all would rather hail a taxi on the street than book a taxicab in advance [34].

Another sector in which the taxi service has a significant role to play is in night-life entertainment. London is the most important city of the UK in terms of entertainment. The city has a quarter of the total expenditures on leisure sector in the country, approximately GBP 9.5 million a year. A high percentage of this expenditure is spent on night activities like drinking in pubs, dining out, gambling and visiting theatres late at night when public transport is scarce [34]. Indeed, a survey conducted by the London Chamber of Commerce in 2006 indicated that the owners and managers of pubs in central London, categorically stated that the biggest issue in the night-time economy is transportation [34]. This is because, there is a mutual benefit between night-time activities and transportation. This is caused by the fact that they depend on the same users, the night-time user, who is highly dependent on their perception of reliability, cost and safety of transportation [19].

Airports are also highly dependent on the Taxi service. They are usually located on the outskirts of cities where it is difficult for travellers commute to the airport using public transport. Therefore, taxicabs are the preferred means of transportation for them, due to the comfort of carrying heavy luggage over a long distance. Furthermore, tourists’ lack of knowledge about commuting and getting around new places is attenuate by the guidance of taxi drivers. Then, the taxi service is provided on airport ranks, established places where taxis can engage passengers [19]. The issue arises due to the increase in the number of flights causing more travellers to use airports. Therefore, the use of the taxi service increases as well, often benefiting a small number of taxi operators who impose higher taxicab fares. Given this fact, authorities are forced to divide the service into smaller companies and owner-taxi taxicabs without joining any operator, offering lower fares for passengers and waiting for users on taxi ranks [19]. This phenomenon is called deregulation, the relaxation of rules allowing more drivers and vehicles to join the taxi service, reducing taxicab rates and increasing the provision of taxis around the city.
2. Background

Fig. 2.1: The main role of the taxicab as a connector between night places and their customers: A taxi at Times Square in Midtown Manhattan, New York City [1].

2.2 Risks to passengers’ safety at the Taxi service

The Law Commission is conducting a consultation about deregulating some aspects the taxi industry in the city of London in order to simplify the process for getting licences for taxi drivers, vehicles and operators, with the purpose of decreasing the cost of taxi fares and increasing the availability of taxi vehicles during off-peak times [37]. These kind of measures might yield dramatic changes the taxi industry. Sweden is a good example: when the taxi industry was deregulated in 1990, the number of taxis and drivers rose significantly. Ten years after deregulation, up to 70% of the taxi market consisted of owner-taxi cabs and large companies had mainly disappeared [38]. This phenomenon is perceived as harmful to the general public because small companies or owner-taxis treat the passenger as a ‘one-time patron’, offering a low quality service because the chance of users returns is almost nil; whereas the staff of large taxi companies are concerned about the users’ experience [19], causing an increase in passengers’ satisfaction and also their perception of safety.

Another risk of deregulation of the taxi industry is the ease with which licences can be acquired. Some measures taken by Sweden authorities were [38]:
• Costs for getting licences were abolished.

• It was not compulsory for Taxi vehicles and drivers to be hired by a taxi operator.

• No geographical limitations for taxi drivers were enforced.

• No timetables for taxi drivers were imposed.

• No specific vehicle model were required.

These measures would facilitate criminals hiding in an increasing number of taxi vehicles: lack of conditions imposed on applicants for a taxi licence might result in the market become flooded with different models of a car type which could confuse the ability of taxi users to recognise legal taxis. Without help from taxi operators, the process of booking a taxi in advance would become more complex. As a result, deregulation could reduce passengers’ perception of safety and local authorities might suffer a setback in their efforts to protect the public interest. In recent years, many other countries have also adopted deregulation. These cases are being analysed by the London authorities to anticipate potential issues and tackle those adequately [37]. However, taxicab services around the world have subtle differences, so the authorities should conduct a thorough analysis, observing the taxi service the context of the local culture of these countries in order to consider which
issues would have a high likelihood of affecting taxi passengers’ safety in the city of London.

Deregulation is not the only action plan taken by authorities that might influence the level of confidence in the taxi service. The UK Government is reviewing various regulations related to the labour market in order to benefit some minorities [31]. One of these regulations is the possibility of not disclosing previous convictions by offenders during employment application processes. Current policies about issuing driver’s licences are based on age, physical condition and criminal record [39]. Indeed, these new regulations establish that no-one will be able to obtain a licence if they have been convicted of murder, a sexual offence or any violent offence in the last ten years [40]. As a consequence, future changes in employment policy might jeopardise the security of taxi passengers.

The major current problem which undermines the perception of safety in the taxi industry is the presence of unauthorised vehicles, providing taxi services to the proper licence to operate the service, commonly known as the illegal taxi market. Cooper [19] conducted a survey among local authorities and identified the relationship between the supply of buses, trains, taxis, and the creation of an illegal taxi market [19]. Indeed, the city of London made public a study that concluded that the taxi service in the city at night is unpredictable and that there is a reason for the outbreak of illegal taxi vehicles picking up passengers on the street, commonly called ‘touting’ [19, 41]. The report emphasized the fact that “the explosion in illegal touting provides incalculable risk in personal safety” [34]. This has indeed given rise to significant concerns among most taxi users about the reliability and safety of the taxi industry in the city.

The above mentioned factors: deregulation, the new labour policy and the illegal taxi market would harm the legal taxi industry in the city and sectors of the economy closely attached to it. According to the London Chamber of Commerce, this sector of the economy generates resources by nearly GBP 5 billion per year in the UK, spending GBP 150 million on combustibles, GBP 40 million on car parts and GBP 12 million on insurance. In terms of journeys, there are approximately 7.7 million journeys per day [34]. Despite the fact that this part of the British economy is strong and the number of incidents still low, Londoners showed concern when hiring a taxi in the street. Passengers expressed their anxiety was one the reasons for avoiding the use of the taxi service “concerns about safety” in the study [34].
2.3 The taxicab secure booking applications

Cooper et al. [19] define three kinds of users of taxi services: the first is the user who hails a taxi in the street; the second is the user who engages a taxi at a rank and the third is the user who books the taxi service in advance. There is a steady increase of users who prefer to use booking taxi services [19]. The traditional approach of a booking system is to have a central office which controls the service, choosing the most convenient vehicle for users. The decision is usually based on the location of the user and the characteristics of taxis operating in the user’s area [19]. Initially, users communicate with central offices by phones, but nowadays mobile phones allow users to use other forms of communication such as SMS or the Internet [19]. Moreover, a public in general has greatly benefited from access to technology: new devices with more capabilities such as smart phones with larger screens, GPS localisers and fast connections to the Internet yield an increase in the number of applications to book a taxicab service [42, 43, 44]. The most common applications belonging to this range are Kabbee, Uber, Hailo and Easytaxi that detect a user’s location using GPS locators of mobiles. After the users’ position has been registered, the system seeks for the nearest taxicab [45], then the application sends information about a driver’s identity and a taxi location to the user [44]. The security of these applications is mostly based on the information provided by the taxi driver when registering with the website of applications, without further control by the authorities.

An early attempt to establish an organised scheme of booking taxi services by local authorities was implemented in the city of London. The authorities created a campaign in 2002 to prevent users from hiring illegal taxis using mobile phones, namely “The Safer Travel at Night” [46]. Three years later, the campaign creators released Cabwise, the first application to book a taxi from a mobile phone. The application sends to mobile users, the phone number of taxicab operators which operate in the same area as users’ location [47]. After that, the location and the user’s phone number are recorded on a database and the system replies by SMS with the phone numbers of the nearest taxi operators. When the user receives the message, they have to communicate with the central office to book a taxi service. Actually, this application is not a taxi booking system because users must call a taxi operator [47]. The use of Cabwise and other pre-booked taxi applications is scarcely adopted by the general public [30].

The applications are highly dependent on the type of regulation adopted on every place. That is the result of the fact large taxicab operators work better with pre-booking in advance users due to they own more vehicles and it is more likely that there is a taxicab near to the passenger, whereas this
mechanism is not efficient for small operators [11]. Therefore, it is crucial to implement a mechanism which guarantees the safety of users without regard to the type of regulation of taxicab industry is currently operating.

2.4 Types of (de)regulated taxicab industries

There are three schemes of regulation [48]:

- Fare regulation: right taxicab fares for users and operators.
- Safety regulation: strict controls to taxicab operation such as vehicle maintenance, security surveillance driver training, etc.
- Entry regulation: provision of a taxicab service.

The fare and safety regulation are subordinates of the entry regulation due to the fact that while on one hand, there is a high provision of the service,
the fares will be decreased and quality service will be increased. On the other hand, when the provision is low, the fares will be increased and the quality service will be affected [10, 48]. The problem arises when local authorities seek to determine the provision of taxicabs. Some countries define following mechanisms [12, 10, 49]:

- Arbitrary number of vehicles providing the taxi service.
- According to the amount of potential customers in the area where is provided the taxicab service.
- The candidate transport operators show the need for the service.
- The authorities establish zones where taxicab companies can operate, then they divide the 'big problem' into 'smaller problems’, this is called ‘sub-leasing system’.
- Establishment of conditions which candidates must meet in order to get a licence.

Pricewaterhouse analysed taxicab entry regulations and defined four types (de)regulation licence requirements [11]:

Type A **Open entry or deregulated system.** It operates one type of licence per vehicle which can be hold for either a driver or an operator. It includes the following features:

- Drivers should enrol operators, but it is not compulsory. They do not need getting a licence for operating a taxicab.
- Lack of strict requirements for getting licences.
- Drivers can transfer themselves to other operators freely if the licence belong to him or her.

Type B **Open entry with company-level qualifications.** Issued licences are only allowed to operators, those hire the drivers of taxicabs. The authorities do not restrict the number of licences per operator but drivers need to get a licence to operate taxicabs.

Type C **Medallion system.** Similar characteristics as type A, except the number of licences is restricted then authorities set strict requirements and licences are transferred usually a high costs.

Type D **Franchise and certificate system.** The most restrictive scheme: operators, drivers and vehicles need a licence to operate:
– A minimum number of vehicles.
– Provision of dispatching service.
– High level of accountability.
– Central offices.
– Driver training program.
– Insurance coverage.

In Sweden, taxicab industry was deregulated since 1963 and they established some controls to avoid collateral effects of deregulation (See section 2.2.2)[10]:

• **Scalability.** Taxi operators must be joined a radio booking centre.

• **Licence operator.** The radio booking centre carries out the regulator authority functions.

• **Quality service.** It also manages quality service controls for drivers.

Yang et al. [10] proposed a supervision system to regulate the taxi industry in China. The system is conformed by four subsystems:

• **Controlling the correct provision of taxicabs.** Average utilisation rate of taxicabs to avoid deficiency on the provision of the service.

• **Taxicab quality service.** Control the driver behaviour and the state of vehicle.

• **Taxicab operation performance.** An efficient use of vehicles to avoid both the unnecessary pollution for excess vehicles operating or a lack of provision resulting an increase of taxicab fares.

• **Real-time supervision subsystem.** Storage trials to monitor the taxicab operation to protect the safe of passengers and drivers.

The scheme will take various concepts from these two experiences to design an authentication system which can be adopted for whichever type of regulatory taxicab industry. Therefore, the scheme will not take into account licences for drivers in order not to exclude A and C taxicab schemes.
2.5 Summary

This chapter presented an overview of the taxicab industry. The importance of maintaining a good perception of safety among tourists in airports; businesspersons working away from the office; customers and workers of the night-life industry. The issues threatening the security of passengers: relaxation of requirements to get a licence, an increase in the illegitimate taxicabs and an adoption of a deregulated scheme may lead to an increase of sexual assaults, robbery, kidnapping express and bad quality service.

It shows some applications that enhance the security of users without great success because they do not take into account the scheme that taxicab industry operates. Therefore, the last part of the chapter provides a comparison of the different schemes of the taxicab industry in order to create a baseline as a foundation for the identification and authentication of taxicabs in the street.
3. TECHNICAL BACKGROUND

The proposed solution is based on three pillars: Authentication using smart cards, public key cryptography and the NFC technology. This chapter is organised as follows:

- Section 3.1 introduces the identification and authentication mechanisms used on smart cards;
- Section 3.2 briefly describes the elliptic curve cryptography and its main advantages;
- Section 3.3 provides an introduction of the NFC technology and its primary uses;
- Section 3.4 concludes the chapter with a brief summary of the security technologies which are the foundation upon which the proposed scheme is being built.

3.1 Authentication

According to Mitchell [50] authentication can be defined as the verification the source of received data or the identity of a party by another. This service is called Entity Authentication. The scheme is primarily concerned with an entity authentication mechanism which can verify a taxicab identity, and it can be used for a great number of persons.

Entity Authentication protocols are based on standards such as the ISO/IEC 9798 Entity authentication [51]. In order to facilitate the design of the scheme, it will adopt an entity authentication protocol used in Smart Cards because they provide a high-level of security and they are specific designed to offer protection a wide range of attacks [52, 29].

Authentication in smart cards is classified as static and dynamic authentication [29]. The former is characterised the same information is used every time the entity is authenticated whereas the latter used different data on every authentication. Another way to conduct an authentication is using symmetric and asymmetric cryptography. The symmetric cryptography has
the advantage of faster performance, ideal for the scarce resources of Smart Cards and asymmetric simplifies the process of key management [50].

3.1.1 Unilateral dynamic symmetric authentication

This way of authentication is defined by a symmetric key shared between the Smart Card and the SCMS. The Smart Card technology which uses this technique is the GSM architecture [20]. The protocol of authentication is challenge-response which the Authentication Centre (AuC) authenticates the SIM card, a smart card, by means of a challenge which the SIM card computes using the shared-key to get the response. The International Mobile Subscriber Identity (IMSI) is a 64-bit number which identifies the SIM card. Every SIM card has a key $K_i$, which is maintained by the SIM card and the Home Network. The cryptographic algorithm A3 in charge of generating the response from the challenge and the key $K_i$ is also held in the SIM card (See figure 3.1).

The security of this method is based on the SIM card and the Home Network are the only parties which know the shared key. Therefore, the Central system has a large database storing the identity and the key of every Smart Card belongs to the system. The security of the protocol is based on the response to the challenge can not leakage information about the key $K_i$ [20]. This is because the response is sent in the clear and a passive attacker can read messages and therefore, he or she can collect a sufficient number of challenge-response pairs in order to analyse and try to deduce the shared-key.

The challenge for key symmetric authentication protocols is the distribution of the key [53]. However, this problem is solve by the SIM card. The SIM card is a smart card, which is a tamper-resistant device holding the Key $K_i$ and the cryptographic algorithms A3 which generates the response to the challenge RAND and A8 which generates the temporal key for the encryption of the session [52].

The use of this technique has a main drawback, it is based on the frequent communication to the Home Network. If the Home Network becomes off-line, the entire system is suspended. It also becomes a problem of scalability, more users and taxis require more Network bandwidth and the cost of the system become expensive due to network rates.

3.1.2 Unilateral static asymmetric authentication

In order to address the drawback, the asymmetric authentication was developed to conduct an off-line authentication because it has the great advantage of asymmetric cryptography: encryption and decryption key are different and
Fig. 3.1: Scheme of the authentication of a SIM card in a GSM Network [3]

from one key cannot determine the other one. This characteristic allows systems to release one key open to public, namely public key and keep the other secret, known as a private key. Asymmetric algorithms such as RSA, ElGamal and Elliptic curve based on ElGamal releases the encryption key as a public and decryption key as a private, whereas Digital Signature algorithms releases the decryption key as a Public, mostly known as a verification key and the encryption key as a private, the signature key.

Finance sector specifies three off-line authentication mechanisms (CAMs) through the EMV standard. They are based on the combination of static and dynamic authentication with asymmetric cryptography: SDA, DDA and CDA [54, 52]. Indeed, asymmetric authentication methods are based on Digital Signatures. The data which contains the identity of the Smart Card is digitally signed using the signature key. After that, the data and its signature are transferred to the Smart Card during the personalisation phase [29]. On one hand, during this manufacturing process, the card is loaded with individual data belongs to every card [52]. On the other hand, the verification key is sent to every terminal on account of ‘decrypting’ the signature of the data contained in the card [53]. There are two approaches to sign data digitally: ‘Digital signature with appendix’ and ‘Digital Signature with message recovery’ [53]. The latter is used when the data and its signature are shorter than the length of the modulus of the Digital Signature algorithm, whereas the former takes the advantages of hashing the data and then, it signs the hash output [53].
This method has two main shortcomings: The first drawback is the system has only one signature key, if the key is compromised, the security of the whole system is compromised as well, then the signature key becomes ‘a global secret’ [52]. The second drawback is the data inside the card is static and it is possible for an attacker to read the data and create a new card with the forged data [29].

Fig. 3.2: An EMV contactless card [4]

A simple certificate hierarchy is used in order to avoid the use of a unique signature key [53]. Therefore, the system has to generate a public/private pair for every group of cards and the verification key has to be held in the card [29]. The process changes slightly, the Master pair Signature/Verification key is at the top and it is created a signature of the Verification key of every group using the Master signature key [55]. The signature of the data is created using the signature key of the group. Therefore, the card will be held: the identification data, a signature of data signed using the signature key of the group, the verification key of the group and a signature of it created by the master signature key. The data and its signature are transferred to the card during the personalisation phase because are unique for every card. However, the Verification key of the group and its signature are transferred to the card during the initialisation phase due to are common to every card belongs the group [52].
3.1.3 Unilateral dynamic asymmetric authentication

The first drawback ‘global secret’ of static asymmetric authentication is addressed by the certificate hierarchy. However, the static method cannot prevent the forgery of the identity. That is the main problem of the SDA authentication, cards are exposed to cloning attacks and their identity is easily forged [54]. For that reason, a challenge-response step was incorporated to improve the authentication mechanism. This fact was defined by Syverson and van Oorshot as one of the six generic goals during formalisation of authentication protocols\(^1\) outlined in [55]. That is the principle behind DDA and CDA authentication mechanisms. However, they required a crypto-processor to sign data making the micro-controller of DDA cards more expensive [54].

The DDA authentication method to verify the identity of the card works as follows [55]:

1. The terminal verifies that the card contains all the data required for the process.
2. The terminal retrieves the Issuer certificate which it attaches the issuer public key.
3. The terminal verifies the Issuer certificate with the ‘trust anchor’ (a verification key of the EMV payment) and extracts the verification key of the issuer.
4. The terminal retrieves the card certificate and verifies it using the issuer verification key. After that, the verification key of the card is stored in the terminal.
5. The terminal generates a challenge of 32 bits and sends it to the card using an APDU-C message.
6. The card creates a signature and returns to the terminal using an APDU-R message.
7. The terminal ‘decrypts’ the signature of the card using the verification key stored on step 4 to verify the authenticity of the card.

Following the above process is easy to corroborate the identity of a card without the need to connect a central server helps save time and resources.

---

\(^1\) Syverson and van Oorshot compiled the most prominent methodologies to design Cryptographic protocols in [56]: BAN logic, GNY logic, VO logic and AT
while ensuring that the authenticity of the identity is not compromised. That characteristic guarantees a stable scalability of the scheme without decreasing the performance of the authentication mechanism.

3.2 Elliptic curve cryptography

A public key cryptography can be evaluated by three parameters: Functionality, security and efficiency [57]:

Functionality: There are three basic operations performed by Public key cryptography: asymmetric encryption, agreement of a shared-key and digital signatures. The encryption of Public Key cryptography is limited by the complexity of operations. For that reason, those algorithms are focus on exchanging a symmetric key in order to encrypt the bulk of data. That is the case for TLS/SSL protocol. The scheme uses Key agreement generation and Digital Signature operations to provide confidentiality between parties and integrity of information respectively.

Efficiency: The third parameter is to calculate how many resources (time, power processing, memory, energy power for constrained devices), the Public-key algorithm consumes according to the required functionality. This point is crucial for the scheme due to the fact there is a time restriction imposed by a functional requirement (See section 4.1.3). Although the time required to execute a digital signature is closely linked to the micro-controller features of the smart card [29], ECDSA algorithm has a better performance during the signing phase whereas RSA digital signatures are faster on the verification phase [5] (See figure 3.3).

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Time in ms</th>
<th>Verify</th>
<th>Signing</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-1024</td>
<td>215</td>
<td>5495</td>
<td></td>
</tr>
<tr>
<td>ECDSA-160</td>
<td>423</td>
<td>423</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 3.3: Comparison extracted from [5] about the performance between 1024-bit RSA and 160-bit ECDSA Digital signatures. The 1024-bit RSA and 160-bit ECDSA schemes provide a near-equivalent level of security according to the figure 3.4.

Security: The security of Public-key cryptography is based on three types of mathematical problems [53, 57]:

- Factorisation of the product of two large prime numbers (RSA problem).
• Discrete logarithm problem (DLP).

• Elliptic curve discrete logarithm (ECDLP).

The perceived security is given by the resources spent to solve a determined length of an instance of the problem. The following are the latest 'records' to break those problems:

RSA. Kleinjung et al. [58] factored a RSA modulus of 768 bits in 2010 by Number Field Sieve (NFS) algorithm in “many hundreds of machines and took almost two years”. Kleinjung recommends to begin to deprecate the 1024-bit RSA [59]. This is due to faster computer with greater power processing and improvements of the algorithms yields factorising big numbers more efficiently.

DLP. Hayashi et al. found the solution of DLP 676-bit prime using 96 cores Xeon 2.83GHz in 33 days in 2009 [59].

ECDLP. Bos et al. solved an ECDLP of a 112-bit key by means of Pollard’s rho method implemented on more than 200 PlayStation 3 game consoles during 100 days in 2010 [60, 61]. The previous record was an instance of a 109-bit prime field in 2003 using the same method [57]. It can be seen that the experts have made very little progress in finding an efficient method to calculate longer prime over elliptic curves.

In order to compare these three methods, some groups of experts in cryptography have proposed tables which establish the perceived security level according to the key length. These tables are based on the security level of a symmetric-key algorithm which it is not affected by a known attack besides a brute force attack which it is possible to calculate the average number of operations in order to search a specific fixed-length key (see figure 3.4).

![Fig. 3.4: Comparison of the level of security according the key length and cryptographic algorithm][6]

<table>
<thead>
<tr>
<th>Security</th>
<th>80 bits</th>
<th>112 bits</th>
<th>128 bits</th>
<th>192 bits</th>
<th>256 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC</td>
<td>160 bits</td>
<td>224 bits</td>
<td>256 bits</td>
<td>384 bits</td>
<td>512 bits</td>
</tr>
<tr>
<td>RSA / Dl. field</td>
<td>1,248 bits</td>
<td>2,432 bits</td>
<td>3,248 bits</td>
<td>7,936 bits</td>
<td>15,424 bits</td>
</tr>
</tbody>
</table>

As it is presented on the table, elliptic curve cryptographic uses shorter keys without decreasing the security level of the algorithm. This is because the arithmetic operations are performed over a discrete set of elements on an elliptic curve called a prime field $F_p$. 


More generally, an elliptic curve is defined in cryptography as the mathematical function \( y^2 + axy + by = x^3 + cx^2 + dx + e \) where \( a, b, c, d, e \in F_p \). If \( F_p \) is represented as a F\(_{2^m}\) field called a binary field. Implementations of elliptic curve cryptography is based on both fields prime and binary fields, commonly represented as ECFieldFp and ECField2m respectively [63]. The elements or points of the field possess some mathematical properties\(^2\) which make possible the use of elliptic curves on cryptography [57]:

- Associativity.
- The existence of an identity.
- The existence of the inverse.
- Commutativity.

The scheme uses two functionalities of EC:

- EC Diffie-Hellman (ECDH) key agreement protocol to make possible the establishment of an encrypted channel between parties.
- EC Digital Signature Algorithm (ECDSA) to guarantee the integrity of the information of the scheme.

3.2.1 Elliptic Curve Diffie-Hellman protocol (ECDH)

The ECDH protocol has as the main goal that is the establishment of a shared-key between two parties over an insecure communication channel. The protocol and its extensions have been standardised in numerous standards ANSI X9.63, IEEE 1363 and ISO/IEC 15946-3 [62]. The key agreement protocol follows below steps (see figure 3.5):

Before the protocol is executed, the parties agree on certain public elliptic curve parameters:

- Finite field \( F_p \)
- Elliptic curve \( E \) over \( F_p \)
- \( P \) is a base point belongs \( E(F_p) \) of prime order \( n \)

1. A selects a random number \( r_a \) as a private value, \( r_a \) is an integer between 1 and \( n-1 \).

\(^2\) The explanation of these properties is outside the scope of this document. However, a clear explanation can be found in [64]
2. A computes its public value $X_a = r_aP$

3. B selects a random number $r_b$ as a private value in the same range as $r_a$.

4. B computes its public value $Y_b = r_bP$

5. A computes $K = r_a(Y_b)$ using its private value and B’s public value and B computes the same value $K$ using the private value and A’s public value $K = r_b(X_a)$

The ECDH protocol provides a high-level security because an eavesdropper only can see the public values $X_a$ and $Y_b$ and he or she cannot calculate $K$ without at least one of private values. Boneh and Lipton proved that the EC Diffie-Hellman problem and ECDLP have the same level of difficulty when $n$
is prime [57]. However, the protocol is gravely impacted by the ‘man-in-the-
middle’ attack which an adversary establishes a communication channel with
both parties at the same time impersonating the identity of the other party
[65]. This problem is addressed by the scheme using certificates to provide
assurance of the identity of the party at the other end of the line (see section
4.2.2).

3.2.2 The Elliptic Curve Digital Signature Algorithm (ECDSA)

The ECDSA provides the functionality of detecting any change the data since
it was issued. It is also standardised in several standards ANSI X9.62, FIPS
186-4, IEEE 1363 and ISO/IEC 15964. The ECDSA has two phases: the
signature generation in which the owner of information signs the data with
his or her signature key $S_a$ generating a signature value $\text{Sign}_{S_a}(message)$
and a verification phase in which the verifier checks the signature using the
verification key $P_a$ and the message.

As ECDH protocol, the ECDSA also has some public parameters:

- Finite field $F_p$
- Elliptic curve $E$ over $F_p$
- $P$ is a base point belongs $E(F_p)$ of prime order $n$
- $P_a$ is the verification key.
- The message.

- Signature phase:

1. A selects a random number $r_a$ as a private value, $r_a$ is an integer
   between 1 and $n$-1.
2. Compute $r_aP = (x_a, y_a)$, $P$ is a point on an elliptic curve, then it
   has two variables: X and Y coordinates.
3. Compute $r = x_a \mod(n)$, $x_a$ is a scalar (it has size but no direc-
   tion).
4. Hash (message). The message is hashed to get a value less than
   $n$.
5. Calculate $s = (r_a)^{-1}(\text{Hash}(message)+S_ar)$. The signature $\text{Sign}_{S_a}(message)$
   includes the pair $r, s$. 
• Verification phase

1. Compute $w = s^{-1} \mod(n)$
2. Compute $u_1 = (Hash(message)w) \mod n$
3. Compute $u_2 = (rw) \mod n$
4. Compute $X = u_1P + u_2Pa = (x_c, y_c)$
5. Verify if $r = x_c \mod(n)$, if both values are equal the signature is correct.

The scheme requires that its components can support EC cryptography. The following are the technologies which provide EC functionality to the elements of the project:

**Smart Cards and NFC tags**: The latest versions of Javacard 2.2.2 and 3.0.4 implement ECDH protocol and ECDSA algorithm [66, 67] with a 192-bit key on prime fields and 193-key on binary fields [66], whereas the technical specification of NFC tags issued by the NFC-Forum specifies only support for a 192-bit key on ECDSA functionality [68].

**Mobile platforms**: Blackberry mobile devices support ECDH in native SDK for Blackberry 10 [69] and following ECDSA instances [70]:

- **ECDSA 192-bit key**: ECDSA P-192/SHA-1
- **ECDSA 256-bit key**: ECDSA P-256/SHA-256
- **ECDSA 384-bit key**: ECDSA P-384/SHA-384

Android OS uses bouncy castle java classes for cryptography support [71]. Bouncy castle has a great range of cryptographic functions such as ECDH and ECDSA [72]:

- **ECDSA 192-bit key**: SHA1withECDSA
- **ECDSA 224-bit key**: SHA224withECDSA
- **ECDSA 256-bit key**: SHA256withECDSA
- **ECDSA 384-bit key**: SHA384withECDSA
- **ECDSA 512-bit key**: SHA512withECDSA

**Back-end Servers**: Java Platform Standard Edition 7.0 supports Elliptic curve cryptography thanks to the provider SunEC which includes ECDH protocol for key agreement and ECDSA for digital signatures [73]. The classes have the same names as Bouncy castle classes.
3.3 Near Field Communication

The NFC protocol was developed by Sony and Philips (now NXP semiconductors) in 2002 with the main goal to simplify the process of authentication using a wireless channel [29]. The protocol operates at 13.56 MHz in various speed rates 106, 212 and 424 kbps over short distances, 4 cm approximately\(^3\). The protocol is interoperable with devices supporting ISO/IEC 14443 type A or B, JIS-X 6319-4 and ISO/IEC 18092 (NFCIP-1) interfaces yielding a high interoperability between NFC-enabled devices with millions of contactless cards around the world [29]. This characteristic makes the NFC-enabled devices more popular thus more devices with NFC built-in become more common. There is an increase of mobile manufacturers steadily which incorporate this technology: 20% of all mobile phones had an NFC module in 2012 according to ABI Research and some experts predicts that these figures will increase more than 50% by 2015 [75]. The increasing tendency among users to own an NFC-capable device makes possible the scheme due to the technology allows the process of authentication of taxicabs in the street and it is available for a vast number of users.

3.3.1 Operation modes

According to the NFC Forum [28], organisation which promotes the use and standardisation of NFC technology, there are three modes of operation:

**Card Emulation mode.** The device adopts the role of a smart card (ISO/IEC 14443 type A or B) and it perhaps may be used on Access Control or e-ticketing systems. Examples:

- *'Touch and Go'* or user less authorisation, a common method used on transportation systems as Oyster Card [76, 75, 23]
- *'Touch and confirm'* or user authorisation mode which user has to verify and certify the transaction such as state-of-the-art mobile payments. [76, 27]

**Peer to peer mode.** They will be able to work as devices exchanging data, creating a secure communication channel. The common application is *'Touch and connect'* that is the connection between two NFC devices as bluetooth devices [76, 74].

**Reader/Writer mode.** The phone begins the action and it usually starts when a user taps his or her mobile near to a tag. The tag then responds by sending an action and content related to that action:

\(^3\) In Reader/Writer mode the protocol can operate in distances up to 20 cm [74]
3. Technical Background

Fig. 3.6: An NFC mobile phone in card emulation mode[7]

**Action: SMS**  
**Content:** Body of a message.

**Action: Call**  
**Content:** Phone number.

**Action: Open a browser**  
**Content:** a URL

'Touch and capture'. The NFC device reads out information of a transponder, useful for adverts on underground stations or places without internet connection because do not require Internet access [76, 77]. 'Touch and link'. Similar than the previous mode, but they requires a connection to an URL on the Internet, then it is necessary to have Internet access [76, 78].

By using this mode, the NFC-enabled devices can read data from a smart card or an NFC tag, making possible for users to verify the identity of a taxicab which carries a smart card and a posterior evaluation of the quality service received by touching a tag inside the taxicab.

The communication between the NFC device with the contactless smart cards is standardised by the protocol ISO/IEC 14443: the device generates an
electromagnetic field which energises the smart card and transmits data from the reader. The transmission from the smart card is done by modulating the load of a carrier with a subcarrier frequency [29]. The upper layer of the protocol stack is defined in ISO/IEC 7816-4, APDU-C for commands from the reader and APDU-R for responses from the smart card [29]. Using the mobile device as a reader, users can easily verify data stored in a smart card such as the identity of the taxicab. Moreover, the smart card is a tamper-resistant device, the scheme trusts that the integrity of the identity will be preserved.

3.3.2 NFC Data Exchange Format (NDEF)

The communication from/to NFC tags were standardised by the NFC Forum by means of establishing specific data formats for a type of applications concatenated on an NDEF message. They defined the following NDEF [74, 79]:

![Structure of an NDEF message](image)

*Text RTD:* It encodes data plain text in UTF-8 or UTF-16 encoding and language identification. It was created for managing metadata for others RTDs [80].

*Uniform Resource Identifiers (URI) RTD:* It communicates a URI from the tag to the reader or vice-versa. The fields are a URI identifier code which
identifies the application such as HTTP, HTTPS, FTP, mailto and the URI field encoding using UTF-8 [81].

*Smart Poster RTD*: The RTD intends to associate URI RTD with its metadata. Furthermore, one of its purposes is trigger actions such as open a browser or sending an SMS [82].

*Signature RTD*: The function of the RTD is to create a digital signature for one or more NDEF messages. It supports following Digital Signature algorithms [68]:

- RSA
- DSA
- ECDSA P-192 SHA-1 with 192-bit key.

Additionally, it establishes the format of the certificate: X.509 or X9.68. Thus the communication between the NFC-enabled device and the NFC-tag can be signed using ECDSA signatures in order to the scheme can verify the integrity and authenticity of the data from the tag.

### 3.3.3 NFC Tag types

The NFC Forum also specifies four types of tags according to their features [83, 84, 85, 86], from the most simple NFC-tag1 until the most complex NFC-tag4 [58]:

**Type 1** Small-size memory devices more than 256 byte but less than 2 Kbyte based on ISO/IEC 14443 type A. They implement 16 or 32-bit digital signatures [74]. They are read/write devices or only read and communicate at 106 kbps.

**Type 2** They possess similar characteristics as type 1 tags with the difference than they do not provide any security mechanism [74].

**Type 3** These tags are more advance than previous tags: the communication speed rate is 212 kbps and it is based on Sony feliCa specification. Memory up to 1 Mbyte and it provides the same level of security than tags type 1 [74].

**Type 4** It is the most secure type, it is a tamper-resistant device and compatible with ISO/IEC 14443 type A or B [29]. It supports up to 64 Kbyte of memory and up to 424 kbps on data transmission. Due to the tamper-resistant characteristic this tag is the most suitable for the implementation of the scheme.
3. Technical Background

3.4 Summary

Technically speaking, the proposed solution is based on three technologies explained in this Chapter: First, the Smart Cards and its dynamic unilateral asymmetric authentication which allows entities to conduct an off-line authentication without depending on a central server making the whole system highly scalable, relates to the ongoing availability of the system and protecting their identities in tamper-resistant devices, Smart Cards and NFC type 4 tags.

Second, the Elliptic curve cryptography, which offers a high security level using shorter keys, ideal for constrained environments such as Smart Cards and NFC tags, and it provides two essential functionalities for the scheme: the digital signature algorithm ECDSA to ensure the integrity of data and ECDH key agreement protocol to provide a shared key to establish an encrypted channel to protect the confidentiality of data.

Finally, the increasingly accepted NFC technology which has become common in most types of mobile devices used by the ordinary citizen and enables them to check the information from a contactless smart card and an NFC-tag using the standard ISO/IEC 14443.
4. THE TAXI AUTHENTICATION SCHEME

This chapter describes the TAXI Authentication scheme as a solution for mitigating the lack of mechanisms for passengers to authenticate a legal taxicab in the street. It describes the requirements, schema and components, which includes:

- In the section 4.1, the security requirements are determined as the foundations for the scheme.

- Section 4.2 presents the interrelation between components and major processes in the system architecture diagram.

- Section 4.3 offers an overview of the main components.

4.1 Security requirements for the taxicab authentication

According to the major issues affecting the security of taxicab passengers described on Chapter 2, I define the following several requirements as starting point. There is two kind of requirements: functional and non-functional requirements. The former are composed of services which are required to meet the needs of the project and the latter address non-related issues, but they are necessary in order to ensure the efficiency and stability of the system such as reliability, usability, implementation and delivery [87]. Two classes of requirements are classified as a functional: User safety and Quality service groups and a category is defined as non-functional.

4.1.1 User safety

The users have a tool to recognise a taxicab which possesses a valid licence before getting into the vehicle. In order to fulfil this requirement is necessary to provide reasonable assurance that the scheme satisfies the following criteria:

Legality: The taxicab possesses a valid licence to provide a taxi service which it is issued by a legal authority or any third-party on its behalf. Moreover, the licence has not been revoked since it was issued.
Taxicab identity authentication: The identity of the taxicab can be corroborated by the user. Then, the user ensures that the taxicab, which he or she is hiring in the street, is the one claimed. Therefore, it must belong to a unique taxicab.

Trustworthiness: The user possesses a trustworthy mobile device with a screen, ensuring that the Licence number belongs to the taxicab and it is valid. The information which appears on the screen is reliable in order to check the identity of the taxicab. The taxicab must be clearly painting the identification (Licence Number) on its doors in order to be easily identified by users.

Authenticity: The identity of a legal taxicab cannot be transferred to another taxicab.

Uniqueness: Any taxicab is not being able to possess two or more identities on the system.

Authentication logs: An evidence of which taxicabs a user has been checked is stored in the system. A third-party can verify them in case of any legal requirement.

Integrity of the taxicab identity: The identity of a taxi cannot change since it was created by the local authorities or a third-party, which it has delegated in it the power and right to enrol taxicabs and issue licences.

Anonymity: The taxicab cannot identify the user during the authentication protocol.

4.1.2 Quality service

The users can assess the taxi service in order to stimulate taxicabs to improve quality service. There are three requirements:

Fairness: Users only can evaluate a taxicab if an engagement of a taxi for hire has been accepted by the driver and the user.

Unlinkability: No-one party can associate the quality service evaluation with the identity of the user whom assesses the service.

Privacy: The information of user enrolment cannot be shared to any entity. All information is released from the Local Authorities must be completely anonymised in order to anyone cannot identify the user.

4.1.3 System’s capabilities and efficiency

The design of the scheme should ensure the operational reliability and a long lifetime to the system. That is required in order to avoid the system fall into disuse.
**Performance:** The process of corroborating the identity and the legality of the taxicab by any user must be done in less than 1000 ms. This is a flexible time, I consider it is sufficient time to conduct the authentication, but not excessive for a customer has to wait before getting into the taxicab. It also prevents some attacks to the scheme (See section 7.1.3).

**Scalability:** The fact that the enrolment of new users and taxicabs should not affect the performance of the system.

**Counter fraud:** A Licence Operator cannot issue more licences than it is allowed without avoiding detection by Local Authorities.

### 4.2 the TAXI System Architecture

The TAXI Authentication scheme is based on the Sweden regulatory scheme [10], which every taxicab is registered to a unique Licence Operator centre. The centre serves as an intermediary between taxicabs and government, the Local Authority or a third-party on its behalf.

According to some authors [10, 11, 12] the number of taxicab companies, which owns a large vehicle fleet, decreases due to the high competition. The taxi market is left to small companies and owner-taxi taxicabs which turn over frequently. Therefore, The scheme only manages licences for vehicles. However, if the taxi industry is regulated by any of the approaches explained on Section 2.4, it just adjusts a few parameters of the system. For example, if the taxi industry is using ‘the medallion approach’, the Licence Operator centre figure becomes a taxicab company and then, taxicab companies are able to issue the number of licences which the local Authorities determine.

The functions of the local authority:

- Issuing licences to licence operators.
- Revoking licences to licence operators.
- User enrolment.
- Managing a database of vehicle licences.
- Managing a database of Licence Operators.
- Publishing updates of valid Licence Operators and revoked vehicle licences to users.
- Maintain a database of quality service evaluations of taxi fares by users.
- Sending quality service evaluations to Licence Operators.
The functions of Licence Operators are:

- Issuing licences to taxicabs.
- Revoking licences according pre-established causes by local authorities.
- Up-to-date the information about issued licences on time.

The functions of taxicabs are:

- Restrict the right to pick up or drop off passengers from either left-hand side or right-hand side but not both sides.

The functions of users are:

- Keep mobile devices constantly charged.
• Install often security patches on their mobile devices

• Install applications only from trust sources.

• Engage the taxi after the TAXI mobile application showed the number of licence or plate and check if the number appearing on the screen matches with the licence number on the taxicab door.

The scheme comprises four elements and seven macro-processes (See figure 4.1). The elements are:

1. The TAXI Local Authority subsystem.

2. The TAXI Licence Operator subsystem.

3. The TAXI Mobile application.

4. The TAXI Fare application.

The subsystems are a part of the Back-office system of the scheme, they provide internal processes which the front-office applications are supported. Its processes are described in the next chapter. Whereas Front-office applications processes, activities which are directly related to users, are outlined in the chapter 6.

The Macro-processes are:

1. Administration of the Licence Operators. 1. The Local Authority manages the responsibility of issuing and withdrawing licences to the Licence Operators.

2. Administration of the licences for taxicabs by Licence Operators. Licence Operators can both issuing licences and withdrawing licences according to legal requirements (see Section 2.3 for common entry requirements) to vehicles providing taxi service. Emphasising the requirement that the vehicle is not registered to another Licence Operator.

3. Up-to-date taxicab licences. Licence Operators have the responsibility of communicating in real time which vehicle licences have been issued and revoked under its supervision.

4. Control of users. The Local Authority manages the user enrolment process and the status of updating revoked vehicle licences and valid licence operators in order to guarantee the trustworthiness of the TAXI Authentication protocol.
5. The TAXI Authentication protocol. The user can check the Operator licence is valid and the taxicab vehicle licence does not belong to revoked licences issued for that operator. It also sends the event of the authentication to the Local Authority in order to track the user if any issue arises.

6. Quality service evaluation. The process allows users to assess the quality service provided by the taxicab preserving data confidentiality at all times.

7. Quality service statistics. The Local Authority can evaluate the Licence Operator using the information extracted from the Quality Service feedback left by users. Furthermore, it can send the quality assessments of every taxicab to the Licence Operator responsible for the licence.

4.2.1 The Key Management System

The main function of the TAXI authentication scheme is the correct administration of the cryptographic keys then as an essential goal is to guarantee that the key management system (KMS) seeks recommendations from international standards. The NIST 800-130 standard defines a set of requirements for KMS [88]. Among considerations for defining and managing keys working on the scheme are:

- The purpose of the key.
- Cryptographic primitive.
- Cryptographic algorithm.
- Owner identifier.
- Key generation.
- Key size.
- Security strength.
- Cryptoperiod.

One of the main objectives of the scheme is to assure the integrity of the information preserving the scalability. For that reason, the scheme provides a three level hierarchy of Digital Signature keys (See figure 4.2), for that purpose: the Local Authority is in charge of the role of the Certification Authority (CA). The scheme has four pair high-level keys. The verification keys
of those are known as ‘trust anchors’ due to they are held in all components as the backbone of trust for the scheme:

- **LAUTH-TAXICABS**: It signs Licence Operator certificates.
- **LAUTH-USERS**: It signs user certificates.
- **LAUTH-LISTS**: It signs licence updates for users.
- **LAUTH-APP**: It signs the TAXI Mobile application.

**Cryptographic primitive**: Digital Signature.  
**Cryptographic algorithm**: ECDSA.  
**Owner identifier**: Local Authority.  
**Key generation**: According to the standard FIPS 186-4[89].  
**Key size**: 386 bits.  
**Security strength**: 192 bits. [90].  
**Cryptoperiod**: 12 years (See figure 4.3).  

The second level is composed by individual keys for Licence Operators and users, OPERID and USERID respectively. For these keys the Local Authority also possesses its own keys OPER-LA and USER-LA.
4. The TAXI Authentication scheme

Cryptographic primitive: Digital Signature.
Cryptographic algorithm: ECDSA.
Owner identifier: Local Authority.
Key generation: According to the standard FIPS 186-4 [89].
Key size: 386 bits.
Security strength: 192 bits [90].
Cryptoperiod: 3 years.

Finally, in the last level every smart card also has an individual key CARD and the NFC devices attached to every taxicab also have individual keys TAXI-FARE. Both of them are signed by the Licence Operators which issue them using its own key OPERID.

Cryptographic primitive: Digital Signature.
Cryptographic algorithm: ECDSA.
Owner identifier: CARD or TAXI-FARE.
Key generation: Internal generation function on the smart card (CARD) or according to the standard FIPS 186-4 (TAXI-FARE) [89].
Key size: 192 bits.
Security strength: 102 bits [91].
Cryptoperiod: 1 year.

The reasons for choosing ECDSA as the digital signature algorithm will be presented on the process 5a, the reasons are motivated by the high performance on constrained devices and efficient use of memory.
The communication between the TAXI Local Authority subsystem and both the TAXI Licence Operator subsystem (see process 3) and the TAXI Mobile application (see processes 5b and 6) is established by means of an encrypted channel using a symmetric shared-key given by the ECDH key-establishment protocol. The keys which are implemented on the scheme provide a protection of data confidentiality during transmissions.

**Cryptographic primitive:** Block cipher.

**Cryptographic algorithm:** Block cipher such as AES, SERPENT or TWOFISH.

**Owner identifier:** the TAXI Licence Operator subsystem or the TAXI Mobile application.

**Key generation:** ECDH protocol.

**Key size:** 128 bits.

**Security strength:** 128 bits [90].

**Cryptoperiod:** A transaction, approximately one or two minutes.

### 4.2.2 The Station-to-station protocol

The communication between parties is conducted by ECDH key-agreement protocol (see section 3.2.1) to get a common temporary key using digital certificates to avoid ‘man-in-the-middle attacks’ (See figure 4.4). After that, the parties use an encryption block cipher to protect the confidentiality of data and ECDSA digital signatures to protect the integrity:

1. **Select random number** $r_a$. The ECDH protocol establishes three public values:
   
   - $P$ is a point on E.
   - $E$ is an Elliptic curve.
   - $n$ is the prime order of $P$.

   The random number $r_a$ is between 1 and $n - 1$ inclusively.

2. **Compute the Public key** $X_a = r_aP$. The initiator generates its public key using the random number and public values. Afterwards, it sends the public key $X_a$, the identity $A$, its digital certificate $CERT_A$ signed by the Local Authority:
   
   - Signature key $LAUTH$-$TAXICABS$ for Licence Operators.
   - Signature key $LAUTH$-$USERS$ for users.
   - Signature key $LAUTH$-$App$ for the TAXI Mobile application.
4. The TAXI Authentication scheme

Fig. 4.4: The Station-to-station protocol
3. **Verification of A’s identity** $CERT_A$. The Local authority verifies the $CERT_A$ using the appropriate trust anchor $AUTH-TAXICABS$, $AUTH-USERS$ or $AUTH-App$. If the Local Authority failed to validate the certificate, the process fails. Otherwise, the fields are checked to corroborate the certificate is still valid. If this is the case, the verification key $P_A$ is extracted from the certificate.

4. **Select random number** $r_b$. The local authority also chooses a random number $r_b$ between 1 and $n - 1$.

5. **Compute the Public key** $Y_b = r_b P$. The Local Authority computes its temporal public key $Y_b = r_b P$ and it sends to A the following data:

   - LOCAL AUTHORITY
   - $CERT_{LOCAL AUTHORITY}$ signed by itself using the appropriate trust anchor.
   - The public key $Y_b$.
   - The signature of the identity of the Local Authority and the public key values $SIGN_{LOCAL AUTHORITY}(LOCAL AUTHORITY, X_a, Y_b)$

6. **Verification of Local Authority’s identity** $CERT_{LOCAL AUTHORITY}$. The A party checks $CERT_{LOCAL AUTHORITY}$ using the correspond trust anchor. It also verifies its fields. After a successful verification, the signature $SIGN_{LOCAL AUTHORITY}(LOCAL AUTHORITY, X_a, Y_b)$ is validated using the verification key attached on the certificate $CERT_{LOCAL AUTHORITY}$. If the signature is validated, the public value $Y_b$ is accepted and A sends to the Local Authority, the signature of public key values as well $SIGN_A(A, X_a, Y_b)$.

7. **Verification of signature** $SIGN_A A, X_a, Y_b$. The Local Authority checks the signature using the verification key attached to the certificate $CERT_A$ validated on step 3.

8. **Compute the session key** $K$. Finally, both parties compute the same session key $K$ independently by means of the multiplication of its private random number and the public key value of the other party:

   - A computes $K = r_a(Y_b)$
   - B computes $K = r_b(X_a)$
4.3 Components

The scheme comprises four main entities:

- The Back-office system:
  - The TAXI Local Authority subsystem
  - The TAXI Licence Operator subsystem

- Front-office applications:
  - The TAXI Mobile application.
  - The TAXI Fare application.

4.3.1 The TAXI Local Authority subsystem

The subsystem is composed by four modules in which stored and manage the information regarding to Licence Operators, users, events and quality service surveys (See figure 4.5).

- Module of administration of Licence Operators. This module manages information about Licence Operators, the Smart cards issued by them
and the certificates used by TAXI Fare application. It also stores the Whitelist of valid Licence Operators and the blacklist of revoked taxi licence certificates.

- **Module of administration of users.** This module manages information about users and updates of valid and revoked certificates needed for the proper functionality of the TAXI Authentication protocol.

- **Module of Authentication events.** The module receives the information about which taxicabs the user have been authenticated successfully.

- **Module of quality service.** Receives the feedback from users about the quality service of taxicab fare and issues the information about those to the Licence Operators. It is appropriate to clarify that quality feedback from users are not manage directly by Licence Operators because in a closed regulated taxicab industry (Type B, C and D), Licence Operators are private companies which are assessed by the feedback as well.

4.3.2 The TAXI Licence Operator subsystem

The functions of the TAXI Licence Operator subsystem are performed by four modules which manages the digital certificates for smart cards and the TAXI Fare application and some functions of quality service assessment (See figure 4.6).

- **Module of administration of Smart Cards.** Initialisation and personalisation of contactless smart cards which store the identity of the taxicab for users to authenticate them using their NFC-capable devices during the TAXI Authentication protocol.

- **Module of administration of NFC tags.** This module manages the process to install the TAXI-Fare application which signs the fare for users who will be able to evaluate the quality of service.

- **Module of administration of certificates.** It stores the signature key OPERID which signs the certificates of both Smart Cards and NFC-tags. It also has the function to up-to-date in real time, the revoked taxicab certificates and establishes communication with the TAXI Local Authority subsystem to inform the new issued certificates.

- **Module of administration of statistics.** This module receives and manages information about quality feedback from customers issued by the Local Authority.
4.3.3 The TAXI Mobile application

The application is composed by four interfaces which executes the process of authentication and manages the quality service assessment (See figure 4.7).

- **Authentication interface.** The interface is in charge to execute the TAXI Authentication protocol which validates the certificates from Licence Operator and Smart Card by means of a chain of trust. The protocol is only effective if the blacklist of revoked taxicab licences and the Whitelist of valid Licence Operators are accurate and up-to-date. It also displays the Licence Number of the taxicab on the mobile screen.

- **Event authentication interface.** The information of authentication is stored in the TAXI Local Authority system, then, this module controls the communication with the subsystem.

- **Up-to-date certificates interface.** It makes possible the synchronisation of valid Licence Operator and revoked taxicab certificates which controls the TAXI Authentication protocol.
4. The TAXI Authentication scheme

- **Service evaluation interface.** The interface sends to the TAXI Local Authority subsystem the quality survey using a secure channel.

The communication between the TAXI Mobile application and the TAXI Local Authority subsystem is supported by a Metropolitan Area Network (MAN) through either a Mobile Network Operator (MNO) or WiMAX operator.

4.3.4 The TAXI Fare application

The application is placed on an NFC tag type 4 and its role is to sign the information from the TAXI Mobile application and the taxi fare with the date and time of execution in order to send to the TAXI Local Authority subsystem via the TAXI Mobile application (See Figure 4.8). The importance of using an NFC tag of this type is because according to technical specifications of the NFC Forum, type 4 is a tamper-resistant device with a high capacity memory, more than 4KB [58], sufficient to store the application and the signature key TAXI-FARE and supports ISO 14443 APDU communication.
4. The TAXI Authentication scheme

An active tag possesses an internal power to maintain an internal clock and it can sign using ECDSA algorithm and supports X.509 certificates [68].

Fig. 4.8: The TAXI Fare application

4.4 Summary

It was defined three groups of requirements: User safety, quality service and system’s capabilities and efficiency, on the basis of the four types of taxicab regulations and previous experiences presented on the Chapter 2.

- User safety.
- Quality service.
- System’s capabilities and efficiency.

Those requirements are addressed by The TAXI scheme which is composed by four components that execute seven processes. The scheme is supported by a certificate hierarchy using X.509 certificates and ECDSA signatures given in the section 4.2.1 (Key Management System). That was possible thanks to various projects and studies described along the document that demonstrate every component can support these features.

It was described the components that conform the Back-office system: The TAXI Local Authority subsystem and the TAXI Licence Operator subsystem and the Front-office applications: The TAXI Mobile application and the TAXI Fare application.
5. THE BACK-OFFICE PROCESSES

This chapter describes the processes running in the Back-office system: the process 1 outlines the management of the Licence Operators licences; the process 2 provides a description of the administration of taxicab licences; the communication of the outcomes of process 2 from the TAXI Licence Operator subsystem to the TAXI Local Authority subsystem is defined in the process 3; at the end the process 7 gives a brief overview of the information included in the statistics of the quality service.

5.1 Process 1. Administration of the Licence Operators

5.1.1 Process 1a. Licence Operator enrolment

This process has the aim to certify that the new Licence Operator complies with local regulations and personnel of the Licence Operator are qualified to operate the TAXI Licence Operator subsystem effectively (see figure 5.1). The steps in this process are based on the current legislation of the city of London to get the licence for Private Hire Vehicles (PHV) operators [92]:

1. **Fill up the registration form.** Prospective firms to get Licence Operator licence are required to complete an extensive registration form that includes some information about the company, its investors and the nominated representative:
   
   - Name of the company.
   - The Registered company number.
   - Full names and ID cards of investors.
   - Nominated Representative.
   - Office address.
   - Phone number
   - Email address
   - Number of Licences

---

1 If the taxi industry operates in either Type A or B regulatory scheme, this field will be omitted.
5. The Back-office processes

Flowchart:
- **Licence Operator**
  - Start
  - 1. Fill up the application form
  - ISO 27001 certification
  - 9. Check the Information Security program
    - 9.1 Physical Access control in the building
    - 9.2 Physical Access control to the Computer Centre
    - 9.3 Key Management System
    - 9.4 Information Security Policies
    - 9.5 Risk Assessment set correctly
    - 9.6 Risk Management process working correctly
    - 9.7 Evaluating Security training program
  - Yes: Proceed to Local Authority
  - No: Recheck the Information Security program

- **Local Authority**
  - 2. Check identities
  - 4. Check bank statement
  - 5. Pre-licensing inspection
  - Yes: Proceed to Third Parties
  - No: Recheck the Information Security program

- **Third Parties**
  - 3. Examine criminal records
  - Police Department
  - Local Authority Planning
  - Planning permission

Legend:
- Start
- End
- Decision point
- Process step
- External entity
5. The Back-office processes

Fig. 5.1: Process 1a. Licence Operator enrolment

- Zone\textsuperscript{2}

2. **Check Identities.** The Local Authority office should conduct a minimum check in order to establish the identities of all investors and the nominated representative on the basis of avoiding the possibility of identity theft.

3. **Examine criminal records.** The Local Authority office informs to the police the identities of those responsible for the proposed operator. After that, national or metropolitan police queries criminal records related to kidnapping, theft, organised crime, sexual assaults and other criminal records which the Local Authority office establishes as a ban from getting the licence.

\textsuperscript{2} If the taxi industry operates in Type D, this field will be omitted.
4. **Check the bank statement.** The proposed operator must supply proof of financial records such as bank statement in order to verify its financial sustainability.

5. **Pre-licensing inspection.** The Local Authority inspects the premises located at the address that appears on the registration form. These have to provide suitable areas in line with the needs of carrying out the regular activities of a Licence Operator.

6. **Planning permission.** The Local Authority planning confirms that the proposed operator is able to use the premises for Licence Operator activity.

7. **Landline telephone number.** This requirement is optional, and it only applies when the Licence Operator is working as a radio booking centre in taxi regulated schemes B, C or D. (See Section 2.4)

8. **ISO/IEC 27001.** This is an unavoidable requirement due to the fact that the Licence Operator is going to manage the TAXI Licence Operator Subsystem, which manages individual keys for taxicabs and the Licence Operator will be support all functions of the Key Management System. Therefore, checking if the applicant Licence Operator is certified on ISO/IEC 27001 or another Information Security Management System standard, it is evidence that the applicant will be maintained a high level of engagement in good practices on Information Security.

9. **ISMS.** On the other hand, the Local Authority must conduct an inspection to validate whether the applicant implements an Information Security programme or not:

   - Physical Access control to the building. Prevent unauthorised individuals to enter the premises of the company.
   - **Access control to the Computer Centre and Information Systems.** Verify physical and logical access controls in order to prevent unauthorised access to the sensitive information.
   - The Key Management System provides an assurance that keys used to manage taxicab licences are properly created, exchanged, storage, used, replaced and destroyed.
   - Information Security Policies are defined according to the business objectives.
5. The Back-office processes

- Risk Assessment process is evaluating the vulnerabilities of critical assets of the Licence Operator and the identification of threats, its probability of occurrence and impact have been evaluated correctly.

- Risk management process is implemented efficiently in order to mitigate the risks found during the Risk Assessment process and appropriate controls are in place.

- Evaluating Information Security training program to assure that everyone knows the functions of their respective security role and regular periodic security awareness training is conducted for all personnel.

10. **Creation of a new account on the TAXI Local Authority subsystem.** An account of the new Licence Operator is created on the TAXI Local Authority subsystem. The new Licence Operator will use the account to create and revoke taxicab licences in real time.

   - Name
   - Certificate ID
   - Nominated Representative
   - Address
   - Landline Telephone Number
   - The number of licences.
   - The starting date.
   - The expiration date.

11. **Generation of Digital Signature keys.** The Local Authority creates a pair of Signature/Verification key for the new Licence Operator OPER. The keys are based on ECDSA algorithm for two reasons:

   - ECDSA algorithm provides a high level of security with shorter keys compared to RSA and DSA digital signatures [53, 51, 29, 93]. This fact allows to save space on the memory of smart cards because it creates small-sized certificates and saves time during the communication with the TAXI Mobile Application due to transmit certificates in less time to the NFC-enabled device in a shorter time.

   2 Field updated on next step.
5. The Back-office processes

- Signing data is faster using ECDSA digital signature algorithm [5, 93, 29]. Therefore, smart cards with constrained resources can create signatures faster than RSA algorithms.

Creation of Public Key certificate. The Local Authority creates the X.509 certificate contained some information about the Licence Operator $CERT_{LICENCE\ OPERATOR}$, the Verification key of the Licence Operator $OPERID$ and the Signature of the certificate by the Local Authority using the signature key $LAUTH - TAXICABS$. The implementation of the X.509 certificate on Smart Cards has been implemented by Henniger et al. [94]. The following are the default fields used by them:

- X.509 version number: X.509v3
- Certificate serial number: Current Licence Operator certificate number
- Issuer name: Local Authority name
- Certificate validity:
  - Not before: The initial date of the licence.
  - Not after: The last date of the licence.
- Signature algorithm identifier: ecdsa-with-SHA384
- Subject public key: Verification key of the Licence Operator.
- Key usage: digitalSignature
- Issuer signature algorithm identifier: ecdsa-with-SHA384
- Signature upon the contents: Digital Signature of the certificate using the Signature key of the Local Authority

12. Transfer the Signature key on a TPM. Due to the fact that the secrecy of the signature key of the Licence Operator is the vital importance, the transportation of the key is doing by means of a Trust Platform Module (TPM) until the place where the Licence Operator has defined to store the key.

13. Storage the signature key on the TAXI Licence Operator subsystem. The Signature key is installed on the TAXI Licence Operator subsystem, which it can be used to sign certificates contained the Verification key of the Smart Cards attached to the taxicabs.
5.1.2 Process 1b. Licence Operator revocation

The local authorities will establish the reasons to withdraw a licence for a Licence Operator according to local regulations [95]. However, the TAXI Authentication scheme requires that the signature keys issued to Licence Operators keep in secret in order to avoid adversaries can sign illegal taxicabs. An efficient KMS requires that the causes of any revocation are specified on the system [88]. Therefore, if any signature key is used to sign forged taxicab licence certificates, the serial number of the certificate contained its verification key is removed from the Whitelist of valid Licence Operators certificates. This process summaries the steps on digital forensic investigations if the reason of revocation is a loss of the key [95] (See figure 5.2).

![Figure 5.2: Process 1b. Licence Operator revocation](image)
1. **Unknown authentication events.** The reception of TAXI Authentication events from unknown certificates, issued by a specific Licence Operator, is evidence that the Licence Operator is not reporting properly the new taxicab licence certificates and the users are at risk.

2. **Plan.** Consider which are the best location to find evidence and appropriate ways to capture that information: The Licence Operator Centre, Smart Phones of users whom authenticate the fraud taxicabs, the Internet, etc. The smart phones and other mobile devices in which the TAXI Mobile application was used to authenticate unknown taxicabs provide an invaluable information to the case.

3. **Capture evidence.** Capture as much information as possible related to the case: CCTV evidence, duplicate Non-volatile and volatile data of servers which the TAXI Licence Operator subsystem is currently running. The collection of network data logs might help investigators to provide clues to analyse malicious activities. It also required to consider service providers of the Licence Operator in the investigation.

4. **Analyse.** During the analysis investigators will try to find the presence of malware, possible infiltration mechanism and exfiltration mechanisms. If they found any evidence, the Local Authority reviews the controls required on the process 1a.

5. **Report.** The generation of a complete report of the examination in order to the competent authorities can have a clear view of the causes which generated the breach.

6. **Final decision.** The Local Authority decides if revoke the licence from the Licence Operator and proceeds to broadcast the revocation event (see process 4b).

5.1.3 **Process 1c. Renovation of a Licence Operator**

The process of renovation of the licence of a Licence Operator is to create a new pair of keys and issue a new certificate before the current certificate expires in order to the TAXI Licence Operator subsystem will be able to create or renew taxicab licences. When the current licence expires all taxicabs must have a certificate signed with the new signature key `OPERID`. (See figure 5.3)
5. The Back-office processes

Fig. 5.3: Relation of lifetimes of Licence Operators and taxicab licences revocation

5.2 Process 2. Administration of taxicab licences

The administration of taxicab licences has three processes: enrolment of a taxicab, revocation of a taxicab licence and renew of a taxicab licence.

5.2.1 Process 2a. Taxicab enrolment

According to several experts this process has many variants depending of the taxi industry regulations [10, 11, 12]. The following steps are based on a deregulated taxi industry in which taxicabs licences are issued frequently and local authorities do not enforce strict requirements to the applicants. If it is required further steps to issue a taxicab licence, it should be placed between steps 1 and 3. The only two requirements imposed by the scheme are in the steps 2 and 3 (See figure 5.4).

1. **Registration form.** The owner of the taxicab fills up a registration form with the information about the vehicle such as model of the car, production year, number of seats and other information requested by local authorities [12]. However, the most important data required are the VIN (Vehicle Identification Number) created by the manufacturer and the number plate issued by the national transportation authority.

2. **Verification previous licences.** The Licence Operator has to be sure that the taxicab has been never issued another licence. The operator can use either the number plate or the VIN of the taxicab issued according to ISO 3779 international standard which contains the World
5. Check the vehicle. After confirmation that the taxicab does not possess any licence, the Licence Operator issues the licence number [11]. The licence number must be painted on the side-door which users get into the taxicab. This requirement is vital to the correct execution of the TAXI Authentication protocol (see process 5a) due to the user must check the licence number displayed on the screen is the same as the licence number.
4. **Creation of an account in the TAXI Licence Operator subsystem.** It will be created an account in the subsystem to identify the taxicab.

- VIN
- Number plate
- Licence number
- Issuing date
- Expiration date
- Vehicle information
- The certificate of the Smart card (registered on step 5)
- The certificate of the TAXI Fare application (registered on step 6).

5. Although there are two options to generate the pair of verification/signature keys: the generation of the pair outside the smart card and then, transfer to the card or using the smart card to generate the keys and retrieves the verification key after that [29]. In this case, the latter is preferred by the scheme because it offers a higher security level in order to the signature key of the card is keeping in secret only for the card. After the card generates the keys, the verification key is transferred to the TAXI Licence Operator subsystem.

The subsystem creates the certificate of the card $CERT_{CARD}$ and it is signed using the signature key of the Licence Operator $OPERID$. Depending on the policies of Local Authorities, the smart cards might be issued with the certificate of the Licence Operator $CERT_{LICENCEOPERATOR}$ during the initialisation phase of the Smart Card manufacturing process or transfer both the $CERT_{CARD}$ and $CERT_{LICENCEOPERATOR}$ on the personalisation phase [29, 52].

- **X.509 version number:** X.509v3
- **Certificate serial number:** Smart card certificate number
- **Issuer name:** Licence Operator
- **Certificate validity:**
  - **Not before:** The initial date of the licence.
  - **Not after:** The last date of the licence.
- **Signature algorithm identifier:** ecdsa-with-SHA1
5. The Back-office processes

- **Subject public key**: Verification key of the smart card CARD.
- **Key usage**: digitalSignature
- **Issuer signature algorithm identifier**: ecdsa-with-SHA1
- **Signature upon the contents**: Digital Signature of the certificate using the Signature key OPERID

6. **Issuing the TAXI Fare application**. The second application on the taxicab is the TAXI Fare application. The application will sign the taxi fare for the quality service evaluation (see process 6). The TAXI Licence Operator subsystem will generate a pair of verification/signature keys for the application TAXI – FARE. The signature key will be transferred to the NFC reader placed inside the taxicab and the verification key will be signed using the key OPERID. The certificate of the card will be stored in the account of the subsystem.

- **X.509 version number**: X.509v3
- **Certificate serial number**: NFC tag certificate number
- **Issuer name**: Licence Operator
- **Certificate validity**:
  - **Not before**: The initial date of the licence.
  - **Not after**: The last date of the licence.
- **Signature algorithm identifier**: ecdsa-with-SHA1
- **Subject public key**: Verification key of the NFC device TAXI-FARE.
- **Key usage**: digitalSignature
- **Issuer signature algorithm identifier**: ecdsa-with-SHA1
- **Signature upon the contents**: Digital Signature of the certificate using the Signature key OPERID

7. Install the smart card and the NFC tag into the taxicab fixedly, in a place which it will be difficult to remove from the vehicle.

The lifetime of licences of taxicabs must be shorter than the Licence Operators (See figure 5.3). The new taxicab licence certificate will be signed using the signature key of the Licence Operator OPERID. If the Licence Operator has two valid Licence Operator certificates, it means it is in a transition time, then the signature key will be used to sign the certificate of the taxicab will be the last key issued.
5.2.2 Process 2b. Taxicab licence revocation

![Diagram showing the process of taxicab licence revocation]

1. **Notice of the revocation.** There are three sources from the notice could be generated: First, Licence Operators can receive a notice of suspension or withdrawal from the Local Authority, in the case, the taxicab is under investigation for any criminal charges. Second, the Licence Operator determines by itself that the taxicab is not obey the rules to provide a high quality service (determined by the Process 7) and revoke the licence. Finally, from the owner of the taxicab when the taxicab is stolen or it is unable to continue providing the service (See figure 5.5).

2. **Include certificate in the blacklist.** The Licence Operator queries the current certificate serial number of the licence of the taxicab to include in the blacklist of revoked taxicabs of the Licence Operator in the TAXI Licence Operator subsystem. After the certificate expires, it
will be excluded from the blacklist to decrease the size of the blacklist file.

3. **Send notification to the TAXI Local Authority subsystem.** The event of revocation is sent immediately to the TAXI Local Authority subsystem.

5.3 Process 3. Up-to-date taxicab licences

5.3.1 Process 3a. Taxicab enrolment

The TAXI Licence Operator subsystem sends to the TAXI Local Authority subsystem, the certificates and information related to new-registered taxicabs the day before of the issuing date which appears on the certificates in order to execute the TAXI authentication protocol properly (process 5b).

1. **Compilation of new certificates.** The TAXI Licence Operator subsystem executes a schedule task to transmit the information of new licensed taxicabs. Then, the subsystems gather the information of the taxicab licences whose period of validity begins the following day (see figure 5.6).

   **Station-to-station protocol.** The Licence operator and the Local authority subsystems execute the ECDH key-agreement protocol to compute a shared-key $K$ (see section 4.2.2). In order to the other party checks the identity, they send their certificates signed by the $LAUTH − TAXICABS$ key.

2. **Send new taxicab certificates.** The Licence Operator sends new certificates of taxicabs with some information (VIN number and number plate) related to them in order to any of them can obtain a new licence from other operator. All data is signed using the signature key OPERID to protect their integrity during transmission.

3. **Validate the signature of data.** The Local Authority corroborates the signature of the data.

4. **Store the information on the database.** The information to be stored on a database.

5.3.2 Process 3b. Taxicab licence revocation

When a taxicab licence is withdrawn, the TAXI Licence Operator subsystem sends to the TAXI Local Authority subsystems the event immediately. The
Fig. 5.6: Process 3a. Taxi enrolment.
communication between the subsystems follows the same protocol than the process 3a.

5.4 Process 7. Quality service statistics

The Local Authority can evaluate the Licence Operator using the information extracted from the Quality Service feedback left by users. Furthermore, it can send the feedback over every taxicab to the Licence Operator which issued the licence. This process can be implemented by secure data transference such as Secure FTP or accessing the Local Operator account on the TAXI Local Authority subsystem via HTTPS.

The information into the system is possible to obtain using the primary key \((UserID, Licence Number, TempID)\) which it is possible consider as a unique value due to the fact the likelihood that a taxicab engages the same user and he or she gets the same temporal ID is almost nil.

- The event authentication date.
- The event authentication time.
- The certificate serial number of Licence Operator.
- The taxicab licence Number.
- The fare charged to the passenger.
- The taxi fare date.
- The taxi fare time.
- Quality service parameters.

5.5 Summary

The TAXI Local Authority subsystem plays the main role in the TAXI Authentication scheme. It generates and stores the 'trust anchors' of the top of the KMS. Its main functions are managing the Licence Operators licences. The subsystems verify that new Licence Operators seek all requirements to get new licences in the Process 1a. It also executes the revocation of those when Licence Operators do not obey local regulations (Process 1b) and establishes the procedure of renovation of licences as well (Process 1c).

The other component of the Back-office system, The TAXI Licence Operator subsystem regulates the taxicab licences according to local regulations.
The main function is to determine the vehicles aspiring to be a taxicab do not possess more than one licence, ensuring the uniqueness of the identity of every taxicab. Therefore, the process of identification of the vehicle by means of the VIN or plate number is the paramount importance for the scheme. After that, the processes of the generation certificates for smart cards and the TAXI Fare application can be done with the certainty that the security of the scheme is not compromised in the process 2a. The process 2b sets the activities when a taxicab licence is revoked.

The process 3 and 7 provide an adequate flow of information between the subsystems. Process 3 is in charge to communicate the issue or withdraw of new taxicab licences and the process 7 is the procedure to inform quality service statistics to the Licence Operators.
6. THE FRONT-OFFICE PROCESSES

Even though the TAXI Local Authority subsystem is a part of the Back-office system, it plays an important role in Front-office applications because it establishes a bridge of communication between those and the internal processes described in the last chapter. This chapter outlines the processes which the users are involved using the TAXI Mobile application and the TAXI Fare application, it includes:

- **Process 4.** The management of users by the TAXI Local Authority subsystem.
- **Process 5.** The interaction between the TAXI Mobile application and the smart card to authenticate the taxicabs.
- **Process 6.** The communication between the TAXI Local Authority, the TAXI Mobile application and the TAXI Fare application to issue the quality service feedbacks.

6.1 Process 4. Control of users

The Local Authority manages the user enrolment process and the status of updating revoked vehicle licences and valid licence operators in order to guarantee the trustworthiness of authentication taxi protocol.

6.1.1 Process 4a. User enrolment

The main goal is to prevent a user can have two or more than two accounts. However, the challenge of identifying a person is really high, and even more so for automated systems which the attendance of the person is not required [97]. There are several restrictions in this field: lack of identity systems in some countries; lack of uniqueness such as people can buy more than one mobile phone or register two different addresses for correspondence; inefficient performance such as expensive readers and costly in-person methods of identification. Therefore, the user enrolment process is based on a common mechanism of user registration which the user can define a username and a
validation message is sent by an SMS to verify the phone number (see figure 6.1).

![Diagram of the process](image)

**Fig. 6.1: Process 4a. User enrolment**

1. **Download the TAXI Authentication application.** The TAXI Mobile application will be available to download from both major application markets. Whereas apple store offers a thorough process of verification against malicious modifications, users which download the application from the android market should be aware of trustworthiness of the marketplace due to the great number of those providing applications [98]. Then, some of them might not offer a strict scrutiny of the software and an adversary can upload a rogue version of the application.
2. **Establishment of a secure channel.** The TAXI Mobile application has the signature using the `LAUTH-APP` key in order to verify the application has not been changed since the TAXI Local Authority subsystem releases the version. After that, the application requests a connection to the TAXI Local Authority subsystem by means of executing the station-to-station protocol. It is important to highlight that the subsystem cannot validate the authenticity of the connection from the application at this early stage and it is a duty of the user to verify the signature of the application is valid.

3. **Capture user personal data.** The user should provide information about his or her personal data, like complete name, mobile phone number, address and other data required by the local authorities. The information is transferred to the subsystem using the secure channel in order to prevent unauthorised access to the personal information. The subsystem sends a random number to the mobile number by SMS to verify the user is a human being and he or she can reach to that mobile number.

4. **Generation of a pair signature/verification key.** Before generating the signature and verification key, the user must enter the random number sent by SMS. Afterwards, the TAXI Local Authority subsystem creates the digital signature keys to the TAXI Mobile application can sign messages (Process 5b and 6) and assign a unique number for identification purposes. The certificate of the user `CERTUSERID` is signed using the signature key `LAUTH-USERS`. The subsystem also sends the actual lists of certificate serial numbers of valid Licence Operators and revoked taxicab licences belongs to them.

5. **Installation of the keys in the TAXI Authentication application.** The signature key `SIGNATUREKEYUSERID`, the user certificate `CERTUSERID`, the verification keys `LAUTH – TAXICABS`, `LAUTH – LISTS`, `LAUTH – USERS` are transferred to the TAXI Mobile Application using the secure channel. The application stores the signature key on a secure storage. It is not enough to set permission only for the application because the android OS leaves whichever application to access files on SD memory by default, then it is necessary to use a secure storage such as the SIM card on mobile phones. For devices which do not posses a SIM card, such as iPad, PDA or tablets, is required the use of secure memories or TPM. If the device does not have any hardware which provides secure storage, operating systems provide a versatile cryptographic functions such as AES-CBC.
of 256 bits [99] and every time the signature key USERID is used, the application must zeroed the part of the memory where the key was held in order to avoid any malicious software might eavesdrop it. The application also stores the verification keys as ‘trust anchors’, the user certificate and lists of certificate serial numbers on a directory where other applications of the mobile cannot make any changes.

6.1.2 Process 4b. Up-to-date licences

The TAXI Local Authority subsystem has two lists: **Whitelist**: It contains the serial number of valid Licence Operators certificates. **Blacklist**: It contains the serial number of revoked taxicab certificates.

![Diagram of the TAXI Mobile application and the TAXI Local Authority subsystem with a process flow for up-to-date licences]

**Fig. 6.2**: Process 4b. Up-to-date licences

1. **Broadcast an event**. The TAXI Local Authority subsystem prepares a broadcast as soon as the Licence Operator informs any revocation of taxicab licence, a new licence operator registration or a Licence Operator licence withdrawn (see figure 6.2). After that the subsystem signs the even using the LAUTH – LISTS key and broadcast to all users.
There is no possible to establish a direct communication to every user because changes must be delivered in the real-time mode.

2. **Store lists.** When the TAXI Mobile application receives an event from the TAXI Local Authority subsystem, the application checks the signature of the event using the verification key $LAUTH - LISTS$. After that, the application proceeds to make the necessary changes according to the event: delete from the whitelist the certificate serial numbers of revoked Licence Operator licences; add to the whitelist the certificate serial numbers of valid Licence Operator licences or add to the blacklist the certificate serial numbers or revoked taxicab licences.

6.2 Process 5. the TAXI Authentication protocol

The TAXI Authentication protocol is composed by two processes: identification and verification of the taxicab (process 5a) and the transmission of the authentication event (process 5b). The user can check the Operator licence certificate is valid and the taxicab licence certificate does not belong to revoked licences issued for that operator. It also sends the event of authenticate taxi to the Local Authority in order to track the user if any issue arises.

6.2.1 Process 5a. Offline authentication mechanism

The mechanism is based on DDA authentication standardised by the EMV guidelines. There are subtle differences aimed faster performance during the execution of the protocol: we can see in the section 3.1.3, where the DDA authentication mechanism is outlined, the reader verifies the certificates as soon as they are retrieved from the card leaving it on stand by and thus introducing a certain degree of inefficiency. As a consequence, the TAXI Authentication protocol validates the certificates when the card is signing the challenge optimising the time required for the authentication. Then, if any validation fail, the protocol will discard the response from the card. Instead of that, it will send a 'Certificate Validation Failure' status to the TAXI Mobile application. The protocol works as follows:

1. The TAXI Mobile Application is always running on the NFC-capable device. Then, the user places the device close to the location where is the contactless Smart Card on the taxicab. The device acting as a terminal begins to send a REQUEST command in order to start the protocol for initialisation and anticollision in accordance to the ISO/IEC
14443 standard. The standard defines two types of communication modes: Type A or Type B [29].

2. The Smart Card transmits the Licence Operator certificate $CERT_{LOCAL\ AUTHORITY}$ to the TAXI Authentication application. The verification of the certificate will be done on the step 6. The key point is this step is to transfer the certificate as quick as possible in order to authenticate the taxicab before the objective time of 1000ms. There are two variables controlling the time of transference: the size of certificate and transmission rate (see figure 6.3).

The former is given by the number of attributes and the length of the key. For that reason, the certificate might contain only the essential attributes enumerated on the step 12 in the process 1a. ECDSA algorithm was selected because its keys are shorter but offers a high level of security. Taking into account these variables the approximate size of the certificate is 1 Kbyte or less [94].

The other aspect, the transmission rate is defined by the ISO/IEC 14443. The standard defines speeds until 847kbps, but the maximum data transmission rate from the card and the NFC-enabled device is 424kbps due to the NFC protocol only supports speeds until 424kbps [74]. The transmission might be executed in three different times, depending on the speed of transference 28ms, 47ms or 85ms at speed rates 424kbps, 212kbps and 106kbps respectively. These times considered the initialisation time of 9ms which Smainger et al. found during the performance evaluation of transmission between contactless smart cards and NFC readers. The speeds will increase in the future due to the fact a release of the newest standard ISO/IEC 14443-2:2010 amended 2012 (Radio signalling interface) and ISO/IEC 14443-3:2011 amended 2012 (Initialisation and anticollision) define Very High Bit rates (VHBR) transmission rates up to 27.12 Mbps [100].

3. Transmission of the certificate of the card $CERT_{CARD}$ takes less time because the length of the key attached to the Smart Card certificate is shorter, maximum 192-bit key length [66].

4. After a successful reception of certificates, the device generates a random number (rnd) and sends it to the Smart Card. The length of the challenge must be 128-bit in order to avoid dictionary and replay attacks.

5. The Smart Card creates an APDU-R to the challenge attaching the next values:
6. The Front-office processes

- The random number (rnd)
- The licence number of the taxicab

The Smart card creates a signature \( \text{SIGN}_{\text{CARD}}(\text{Licencenumber}, \text{rnd}) \) using ECDSA algorithm. This is the most critical part of the TAXI Authentication protocol because it is the step that takes longer. The time it takes is variable and depends on the characteristics of the Smart Card. The key point is that the Smart Card must be Javacard version 2.2 or higher which support ECDSA digital signatures [101]. Rohde et al. presented a comparison between digital signature algorithm performances on Smart Cards, ECDSA signatures took a considerable less time than RSA algorithm, 427ms [5]. Furthermore, the latest technology on ICC, the model P5CD081 of NXP takes 30ms to sign data using a 163-bit key [102].

6. While the Smart Card is processing the challenge. The device can verify the authenticity of certificates and validate they are not in blacklists. The first certificate to review is the Licence Operator using the Verification key of the Local Authority (LAUTH-TAXICABS). Rosati et al. show that verifying signatures of 384-bit keys does not take more than 14ms on a on Blackberry Bold 9700 mobile phone.

After that, if the signature of the certificate is valid, the TAXI Mobile application checks the following fields:

- Issuer name: the name matches with the Local Authority
- Certificate validity: the time is between the starting date and the expiration date.
- Key usage: the certificate is for creating digital signature.
- Certificate serial number: It is not empty.
- Subject public key: It is not empty.
- Subject Name: It is not empty.

If any of verifications fails, the process of authentication the taxicab will be interrupted displaying the correspondent error message to the user.

7. Due to the reduce number of Licence Operators, the serial number of valid certificates are stored in the TAXI Mobile application. This is a Whitelist and it must contain the certificate serial number in order to the authentication protocol remains on course.
8. After validating that the Local Operator certificate is valid, the TAXI Mobile application proceeds to verify the Smart Card certificate. The process is similar as it was presented on the step 6. The field ‘Signature upon the contents’ is verified using the verification key of the Licence Operator (Subject public key) extracted in the step 6.

- **Issuer name**: the name matches with the Licence Operator name (Subject Name on the Local Authority certificate).
- **Certificate validity**: the time is between start date and expiration date.
- **Key usage**: the certificate is for creating digital signature.
- **Certificate serial number**: It is not empty.
- **Subject public key**: It is not empty.

9. Due to the large number of registered taxicabs, the taxicabs with a revoked licence is stored in the CRL inside the TAXI Mobile application. The certificate serial number is compared with all found on CRL. If there is no matches, the process of authentication is continuing normally.

10. The Smart Card sends the APDU-R which it was prepared on step 5 to the device.

11. The TAXI Mobile application verifies the signature using the key found on the Smart Card certificate.

12. If all steps are successfully executed, the TAXI Mobile application shows the licence number on the screen of the device.

13. The user has to validate that the licence number matches with the licence number of the side-door of the taxicab. If the user decides to take the taxicab pushes a button HIRE and an event is created in order to send to the TAXI Local Authority subsystem. The followings are the fields included in the event:

- UserID.
- Date of the reception of this event.
- Time of the reception of this event.
- The licence number of taxicab.
- Random Number (rnd).
6. The Front-office processes

• Signature from the card.

At the end of the process 5a, the taxicab is authenticated by the TAXI Mobile application.

6.2.2 Process 5b. The Authentication event

The goal the process is transmitted the information of the authentication event to the TAXI Local Authority subsystem without compromise the confidentiality of the quality service feedback given by the user or the privacy of user data. This part of the process does not have the same restrictions of time of 1000ms (see figure 6.4).

1. **The user selects the HIRE option.** The user confirms that he or she is taking the taxicab and the Licence number on the screen of the mobile device is the same as the Licence Number which appears on the side-door of the taxicab.

The TAXI Mobile application and TAXI Local Authority subsystem exchange certificates, \( CERT_{USERID} \) and \( CERT_{USER-LA} \) respectively. Both certificates are signed by the trust anchor LAUTH-USERS. Then, they conduct the station-to-station protocol (see section 4.2.2) in order to get the session key \( K \) which is used to encrypt the messages between parties.

2. **Sent an authentication event.** The TAXI Mobile application creates an event attaching the following data:

   • The certificate serial number of Licence Operator.
   • The licence number of taxicab.
   • The random number (rnd).
   • The signature from the card.
   • The signature of the data using the signature key belongs to the user the signature key \( USERID \).

3. **Validation the signature from the card and user.** The Local Authority checks the signature of the data to guarantee the integrity of the information using the \( USERID \) public key. After, the certificate belongs the card is retrieved from the database using the Licence number of the taxicab. The verification of the signature from the card is doing by employing the Random number (rnd), the Licence number and the verification key of the card found on the certificate. The reason is to avoid fake registration events from dishonest users.
6. The Front-office processes

Fig. 6.3: Process 5a. the TAXI Authentication protocol
Fig. 6.4: Process 5b. The Authentication event
4. **Store in the database.** The information from the event, the time and date are stored in the TAXI Local Authority subsystem with the aim of providing an audit record for a third-party.

5. **Send confirmation.** The subsystem creates a random temporal identification TempID in order to the TAXI Mobile application can perform the feedback of the taxi fare without revealing any personal data. This is due to the fact the taxicab will not be able to identify the user. The temporary identification is sent using the secure channel.

6. **Store the confirmation on the TAXI Mobile Application.** The temporal identification is stored on the device to conduct the quality evaluation of the taxi fare.

6.3 **Process 6. The Quality service evaluation**

Users should assess the service provided by the taxicab with the assurance that his or her information is maintained confidentially. The process uses the temporal identification TempID given by the TAXI Local Authority subsystem in the process 5b. The communication between the TAXI Mobile application and the TAXI Fare application is provided by means of the NDEF: Text RTD, which transport the data and a Signature RTD which transport the digital signature that ensures the integrity of data is protected (see section 3.3.2). The user has to touch the NFC reader inside the taxicab after the driver issues the taxi fare ticket and the quality service survey appears on the screen of the user.

1. **Send Identification.** In the previous process, the TAXI Mobile application received the TempID from the TAXI Local Authority subsystem. The user need to tap the NFC reader located inside the taxicab using the NFC-enabled device, after the taxi fare is confirmed by the driver at the end of the journey. Then, the TAXI Mobile Application sends the TempID to the TAXI fare application. This TempID protects the user against any attempt to identify him or her.

2. **Generation of the taxicab fare event.** The TAXI fare application signs the following information: Taxi Fare, TempID, the date and time when the event is created using the signature key of the taxicab for evaluation TAXI-FARE. The information and the signature are sent to the TAXI Mobile application: 

\[ \text{SIGN}_{\text{TAXI-FARE}}(\text{TempID, Licence Number, date, time, Taxi fare}) \]
Fig. 6.5: Process 6. The Quality service evaluation
3. **The user assesses the quality service.** The TAXI Mobile application shows the information about the taxi fare and quality service survey on the screen. The user validates the Licence Number of the taxicab. The user can evaluate the service after the journey is finished. The Local Authorities should establish a maximum time when users might assess the taxicab service.

Afterwards, The TAXI Mobile application and the TAXI Local Authority subsystem create an encrypted channel by means of establishing an instance of station-to-station protocol (see section 4.2.2). After that both entities agree on a secret key $X$ which can use to encrypt the information using a block cipher algorithm such as AES.

4. **Send the quality service survey.** The TAXI Mobile application transmits the information about evaluation from the user. The information is signed to prevent any change during transmission:
   - The $UserID$.
   - The licence number of taxicab.
   - The $TempID$.
   - The charged fare.
   - The date from the NFC-tag.
   - The time from the NFC-tag.
   - Quality service parameters.
   - The signature from the TAXI fare application.
   - The signature of the data from the TAXI Mobile application.

5. **Validation the signature from the TAXI fare application.** The Local Authority retrieves the certificate of the TAXI fare application using the Licence number of the taxicab. The verification key $TAXI-FARE$ listed on the certificate is used to verify the signature: $\text{SIGN}_{TAXI-FARE}(\text{TempID}, \text{Licence Number}, \text{date}, \text{time}, \text{Taxi fare})$. Taking into the account that the TempID is a random number and the likelihood that a user has the same TempID twice is almost nil. It is not possible that a user can replay the same signature from the TAXI fare application more than once and therefore the user could not assess a taxicab before the driver issues the taxi fare ticket. Finally, the information of the quality service survey is registered on the TAXI Local Authority subsystem.
6.4 Summary

The TAXI Local Authority issues the TAXI Mobile application to the application markets. The user creates their respective accounts in the scheme using the application in the process 4a. The subsystem broadcasts the up-to-dates of revoked taxicabs and valid Licence Operators in the process 4b.

The TAXI authentication protocol is executed by the TAXI Mobile application and the SIM card attached to the taxicab. The user initialises the protocol using his or her NFC-enabled mobile device as a reader. The protocol is an implementation of the off-line asymmetric authentication with subtle differences aiming to reduce the execution time as much as possible in the process 5a. The process 5b establishes the communication with the TAXI Local Authority in order to store the authentication logs generated by the TAXI Mobile application, generating a temporary ID for the quality service survey to protect the privacy of users and identify possible frauds or errors committed by Licence Operators.

The TAXI Fare application is a stand-alone application installed on a tamper-resistant NFC tag which needs a constant source of power in order to maintain an internal clock. It receives information from the taxicab fare calculator and the TAXI Mobile application in the process 6.
7. SECURITY ANALYSIS

The first part of this chapter describes which processes of the TAXI Authentication scheme fulfils the requirements listed on the beginning of Chapter 4. The major issues which affect the perception of safety in the Taxi industry described on Chapter 2: crimes against taxicab passengers, the illegal taxi market and a decrease in the taxicab quality service are addressed the other section of this chapter.

7.1 Analysis of the system requirements

The main goal of the project is to provide an authentication mechanism which allows passengers to check taxicab licences efficiently in the street, both in order to prevent illegal taxicabs could endanger the integrity of passengers and detect legal taxicabs used by criminals. Another goal is to provide a reliable quality service to increase the perception of safety in the taxicab service. Apart from that, the last set of requirements aims to guarantee the adoption of the scheme by the community.

7.1.1 User safety

The users have a tool to recognise a taxicab which possesses a valid licence before getting into the vehicle. In order to fulfil this requirement is necessary to provide reasonable assurance that the scheme satisfies the following criteria:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Legality</td>
<td>The licence of a taxicab is issued by Licence Operator (process 1) which it also has a licence to issue taxicab licences. If either the licence of the taxicab or the Licence Operator is revoked before the expiration date, the processes 2 and 3 guarantee all users will be aware of the issue as early as possible.</td>
</tr>
</tbody>
</table>

Fig. 7.1: Analysis of the user safety requirements
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Taxicab identity authentication</td>
<td>The TAXI Mobile application cannot stored the verification key of every smart card because the system would flood up-to-dates every time there is a new taxi-cab. Instead, the application has the verification key LAUTH-TAXICABS which is used to validate the Licence Operator certificate that it retrieves from the smart card. After that, the application uses the verification key OPERID on the certificate to verify the smart card certificate. Finally, the verification key attached to the smart card certificate is used to corroborate the challenge sent by the application.</td>
</tr>
<tr>
<td>3. Trustworthiness</td>
<td>The TAXI Mobile application is digitally signed by the Local Authority using LAUTH-APP key. Then, it cannot be changed from any attacker without detection. The application receives up-to-dates signed by the TAXI Local Authority subsystem using LAUTH-LISTS, then any modification of the Whitelist to include a rogue Licence Operator or the blacklist to delete any banned taxicab will be detected by the application.</td>
</tr>
<tr>
<td>4. Authenticity</td>
<td>The licence is represented by the digital certificate generated by the Licence Operator using the verification key created by the smart card. These verification keys are unique and they are transmitted attached to their respective certificates to the TAXI Local Authority subsystem. In the process 5b when the TAXI Mobile application sends the authentication event to the subsystem. The subsystem validates the challenge with the stored verification key to detect if the identity of the taxicab is genuine from what it was reported by the Licence Operator. Moreover, two certificates cannot have the same serial number on the TAXI Local Authority subsystem. In the case the Licence Operator tries to register a taxicab with a current licence number in the process 3, the Local Authority will detect and inform the error.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Processes</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>5. Uniqueness</strong>&lt;br&gt;Any taxicab is not being able to possess two or more identities in the system</td>
<td>The system has the restriction of one licence for every vehicle to avoid unauthorised transferences of identities to other vehicles. That is the reason to issue one smart card for licence and the policy of picking users up for one-side of the taxicab exclusively. The scheme provides a strict verification of a vehicle can not be issued with more than one licence. The initial step on process 2 checks if the vehicle which is applying to get the licence has been issued with a licence using the plate number and VIN numbers, unique identifiers of every vehicle.</td>
</tr>
<tr>
<td><strong>6. Authentication logs</strong>&lt;br&gt;An evidence of which taxicabs a user has been authenticated is stored in the system</td>
<td>The TAXI Mobile application sends to the TAXI Local Authority subsystem an event containing:</td>
</tr>
<tr>
<td></td>
<td>• The Licence operator certificate serial number</td>
</tr>
<tr>
<td></td>
<td>• The Licence Number of the taxicab</td>
</tr>
<tr>
<td></td>
<td>• The challenge</td>
</tr>
<tr>
<td></td>
<td>• The response from the smart card</td>
</tr>
<tr>
<td>The communication between entities is encrypted to protect the confidentiality of the data and digitally signed to protect the integrity of information.</td>
<td></td>
</tr>
<tr>
<td><strong>7. Integrity of the taxicab identity</strong>&lt;br&gt;The identity of a taxi cannot be changed</td>
<td>The identity of a taxicab is issued by the Licence Operator by means of a licence number and a digital certificate in the Process 2a. They are transmitted to the TAXI Local Authority subsystem in the process 3a. The digital certificate only can change when it is expired, but the licence number cannot be changed and it is permanent linked to the identity of the taxicab as a vehicle, plate number and VIN, in the TAXI Local Authority subsystem.</td>
</tr>
<tr>
<td><strong>8. Anonymity</strong>&lt;br&gt;The taxicab cannot identify the user during the authentication protocol</td>
<td>During the TAXI Authentication protocol, the contactless smart card transmits both the Licence Operator and the smart card certificate to the NFC-enabled device belongs to the user. However, the device only sends a random number to Smart Card in order to be signed using the smart card signature key. Thus any information belongs to the user is disclosed. After that, the communication between the TAXI Mobile application and the TAXI Local Authority subsystem is encrypted to inform the authentication event protecting the user’s identity.</td>
</tr>
</tbody>
</table>
7. Security Analysis

7.1.2 Quality service

Users can assess the taxi service in order to stimulate taxicabs to improve quality service. The scheme has to provide three principles to guarantee this requirement will be satisfied.

Fig. 7.2: Analysis of the quality service requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Fairness</td>
<td>During the last step of the TAXI Authentication protocol (process 5b), the TAXI Local Authority subsystem sends a temporal ID TempID to users in order to identify themselves to the TAXI Fare application on the quality service evaluation process. At the end of the process 6, the Local Authority verifies the signature from the TAXI Fare application contains the Temporal ID to establish that the user got a taxi ride on the taxicab identified with the reported Licence Number during the protocol. This mechanism also provides protection against multiple evaluations of the same journey because the tempID is a random number and it is highly improbable two journeys of the same user on the same taxicab have the same tempID.</td>
</tr>
<tr>
<td>2. Unlinkability</td>
<td>The taxicab does not identify the user on the authentication protocol (Process 5a) and the user uses a temporal ID as an identity during the quality service evaluation process (Process 6). Therefore, the feedback cannot be related to the user during the journey. This mechanism also provides protection against multiple evaluations of the same journey because the tempID is a random number and it is highly improbable two journeys of the same user on the same taxicab have the same tempID.</td>
</tr>
</tbody>
</table>
### Security Analysis

#### Requirement

**3. Privacy**

The information of user enrolment cannot be shared to any entity.

When the information is captured by the system on the Process 4a, the TAXI Mobile application creates a secure channel to the TAXI Local Authority subsystem by means of encrypting data and digitally signed them.

Additionally, as it was presented before, the identity of the user is never revealed during the TAXI Authentication protocol and quality service assessment, process 5 and 6 respectively.

Furthermore, as a part of the process 7, the Local Authority distributes the quality service statistics, the released information omits the identification of users or any data which could lead the Licence Operator or taxicab owner/driver to identify the user.

#### 7.1.3 System’s capabilities and efficiency

The design of the scheme should be ensured operational reliability and a long lifetime to the system. The assurance of the adoption of the system by the community is given by the below key drivers:

**Fig. 7.3:** Analysis of System’s capabilities and efficiency requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Performance</strong></td>
<td>The TAXI Authentication protocol authenticates a taxicab in less than 1000 ms in the process 5a. To attain that objective, a modification of the DDA protocol is implemented: the TAXI Mobile application retrieves the certificates of Licence Operator and the card. Then the application validates both certificates while the card is generating the signature for the challenge, saving time because the signature of the challenge is the step which takes longer. However, this time has to be reviewed frequently because it must be able to validate the taxicab licence by the application, but protection against relay attacks should be maintained at all times.</td>
</tr>
</tbody>
</table>
2. Scalability
The fact that the enrolment of new users and taxicabs should not affect the performance of the system.

3. Counter fraud
A Licence Operator cannot issue the same licence to two or more taxicabs because every licence is linked to a certificate attaching a verification key which only one smart card is holding its corresponding signature key. During the process 3a, the Licence Operators send to the Local Authority, the digital certificates of smart cards with its correspondent verification keys. Then, at the end of the process 5b when the Local Authority checks the signature provided by the card after a successful authentication of a taxicab, two cards are not be able to sign authentication events which can be validated using the same verification key.

A summary of which processes fulfil every requirement can be found in the figure 7.4. It is important to highlight that even though the process 1c (Renovation of Licence Operator licences) is not required for fulfilling any requirement, it is necessary during the transition time when a Licence Operator is changing its signature/verification keys.

7.2 Analysis of real-world crimes

Having considered the generic security requirements, we now analyse the issues affecting the perception of safety in the taxicab industry presented in the Chapter 2.
### 7. Security Analysis

#### Fig. 7.4: Requirements Vs Processes

<table>
<thead>
<tr>
<th>Administration of the Licence Operators</th>
<th>Quality service statistics</th>
<th>Quality service evaluation</th>
<th>The TAXI Authentication protocol</th>
<th>Control of users</th>
<th>Up-to-date taxicab licences</th>
<th>Administration of the licences for taxicabs</th>
<th>System's capabilities and efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1b</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2a</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2b</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3a</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3b</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4a</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4b</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5a</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5b</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>7</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- **1. Legality**
- **2. Taxicab identity**
- **3. Trustworthiness**
- **4. Authenticity**
- **5. Uniqueness**
- **6. Authentication logs**
- **7. Integrity of the taxicab identity**
- **8. Anonymity**
- **1. Fairness**
- **2. Unlinkability**
- **3. Privacy**
- **1. Performance**
- **2. Scalability**
- **3. Counter fraud**

**User safety**

**Quality service**

**System's capabilities and efficiency**
7. Security Analysis

7.2.1 Kidnap a customer ‘express kidnapping’ and lure criminals into a taxi for robbery or sexual assault

As it has been put forward, one of the major issues endangering the taxicab passengers is the presence of criminals on taxicabs. As Gambetta et al. [9] pointed out mimicking the signals of trustworthiness of a legal taxi “camouflage” is the most common way for criminals to deceive their victims. In order to mitigate that issue, the scheme provides controls to prevent criminals can imitate a legitimate taxicab. Indeed, it is relatively straightforward make a vehicle looks like a taxicab\(^1\). Therefore, the only mechanism that prevents the crime is the smart card held by the authorised taxicabs. Following are some low level attacks which adversaries might execute in order to impersonate the identity of a legal taxicab:

**Forging the identity of a taxicab.** For an attacker could copy the identity of a taxicab, it will be necessary to copy the data of the smart card which contains the signature key CARD. The smart card is the only entity which possesses the signature key and it is a tamper-resistant device which includes several controls to prevent an unauthorised copy of data [52]. Nevertheless, attackers do not see the need to extract the signature key if they could generate all possible signatures for any challenge on the TAXI Authentication protocol. However, this option is almost impossible because the challenge sent by the TAXI Mobile application when executes the TAXI Authentication protocol is a 128-bit number which generate \(2^{128}\) different responses, having a 128-bit challenge is good and in-line with the best practices, for that reason this option is not viable for attackers.

Another way to forge an identity is by removing ‘stole’ the smart card of the taxicab. Although in the last step of process 2a, the smart card is placed on a secure place, there is still a possibility that the device could be removed from the legitimate taxicab. The ‘stolen taxicab’ will be unable to work thus it will be quickly detected by the driver and the up-to-dates in real time will inform the users about the issue, process 3 and 4. However, if any passenger is mugging into the taxicab, the trials of victim’s authentication (process 5b) will be stored on the TAXI Local Authority subsystem, making easily for authorities to detect criminals. This situation makes the attack costly for criminals whom have to steal a taxicab every time they lure for robbery.

\(^1\) The level of difficulty depends on the taxi regulation scheme: open-regulated schemes which do not restrict the use of conventional brands as taxicabs are easier to mimic than types B and D schemes which could require specific car models such as “the Hackney carriage” or “black cabs” in the city of London [103]
If attackers can compromise the user’s mobile devices is another method that attackers try to execute in order to deceive users. The application is digitally signed using the LAUTH-App key facilitating the detection of any unauthorised modification of the TAXI Mobile application. But it is also true that a rogue application could manipulate the data and it could display any Licence Number on the screen. For that reason, it is paramount for the system, users should download the application from well-known application markets and up-to-date their mobile OS regularly to reduce the vulnerabilities which could be exploited by criminals. An installation of an anti-virus could help OS to detect several kind of malware as well. Developers also should seek recommendation for secure application development such as SDLC or more specific recommendation for mobile applications when develop the application [71].

Deceive the system by modifying the identity of a taxicab on the authentication event. If the case that criminals can manipulate the communication between the NFC-capable device and the smart card 'man-in-the-middle', highly feasible when data are encoded using Manchester code but less possible when Miller codification is used [104]. Nevertheless, there is little attacker can do to deceive the NFC-enabled device because the TAXI Mobile application checks the information originated from the smart card using the signature and whichever alteration such as the licence number of the taxicab will be detected by the application due to the fact that all certificates are digitally signed.

Attackers will also try to manipulate the transmission of the authentication event, but the integrity of the information between the TAXI Mobile application and the TAXI Local Authority subsystem is protected using an ECDSA digital signature signed by the USERID key and confidentiality by the encryption using a block cipher symmetric algorithm with a 128-bit key.

Deceive a user to accept the identity of a taxicab when its licence was revoked or expired. The TAXI Mobile application checks the fields of certificates from the smart card on the process 5a. It extracts the Certificate serial number of Licence Operator and then, it compares whether the number is included into the Whitelist of valid Licence Operator certificates or not. On the one hand, in the case of the application could not find it into the valid certificate repository, the process of authentication will fail. On the other hand, the process will continue to check the Smart Card certificate. First, the signature is verified. Secondly, the process determines
if the certificate is still valid in accordance to the certificate validity dates. Finally, the serial number is compared against the blacklist of the Licence Operator to find whether the licence was revoked before the expiration date. If the adversary tries to modify any field, the application cannot verify the signature of any certificates and the process will inevitably fail.

**Relay attack.** Deceive a user to accept the identity of another taxicab. The adversary transmits the authentication messages on the *TAXI Authentication protocol* to a valid taxicab during a relay attack (See figure 7.5). This kind of attacks impacts significantly DDA authentication mechanisms. Indeed, the attacker does not need to transmit all messages from the NFC-enabled device, he or she only needs that a valid Smart Card response the challenge as ‘an oracle’. Other information is static such as the digital certificates and they can be copied easily. This is the reason SDA authentication mechanisms are avoided for secure application implementations (See section 3.1.3). In order to mitigate the attack, the scheme has a restriction of 1000 ms which is a reasonable time to execute the first part of the TAXI Authentication protocol (process 5a) and avoid relay attacks, thanks to high delays in mobile communications: 500 ms or more in WiMAX [105]. However, new advances on the telecommunication field will decrease the delay in mobile channels forcing authorities to decrease the maximum time allowed for the process 5a, a requirement of 75ms between end-to-end applications in LTE networks [106].
7. Security Analysis

Fig. 7.6: Statistics of overlapped journeys of the same taxicab licence number

<table>
<thead>
<tr>
<th>Licence Operator Certificate Serial Number</th>
<th>Taxicab Licence Number</th>
<th>Event Authentication date</th>
<th>Event Authentication time</th>
<th>Test fare date</th>
<th>Test fare time</th>
<th>Quality Service parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234-7890</td>
<td>P0X-1234</td>
<td>02/08/14</td>
<td>07:34:32</td>
<td>03/08/14</td>
<td>07:15:12</td>
<td></td>
</tr>
<tr>
<td>1234-7890</td>
<td>P0X-1234</td>
<td>02/08/14</td>
<td>07:20:45</td>
<td>03/08/14</td>
<td>07:20:35</td>
<td></td>
</tr>
<tr>
<td>1234-7890</td>
<td>P0X-1234</td>
<td>02/08/14</td>
<td>07:16:78</td>
<td>03/08/14</td>
<td>07:15:40</td>
<td></td>
</tr>
</tbody>
</table>

7.2.2 Operate an illegal taxicab ‘touting’

Another issue which is important to highlight is the countermeasures against the illegal taxi market. Illegitimate taxicab operators outside the scheme have to use the same strategies as criminals presented in the before section. However, a dishonest Licence operator or taxicab owner might try to execute the following attacks taking advantage from they already operate some legal taxicabs:

**Operate a taxicab with a fake taxicab licence.** Creating an identity is another way to deceive the system. The attackers should initialise and personalise a smart card with a fake licence number. Although they might create the certificate, they need the signature key of the Licence Operator OPERID in order to sign it. As seen in the process 1a, the Licence Operators must comply with a compulsory-operation requirements which, among other things, include an inspection of the Information Security program which ensures the signature key OPERID is appropriately protected.

**Duplicate a licence for two or more taxicabs.** Generate the signature of the card outside and copy the signature to two different cards. Despite the fact that an adversary could implement the attack successfully, the scheme has another control to detect this kind of attacks. On process 7, the statistics will show various overlapping journeys of the same Licence number (See figure 7.6). This abnormal behaviour indicates an irregularity in the correct management of the taxicab licences by the Licence Operator.

7.2.3 Undermine the quality service of the scheme

Evaluate a service without getting in a taxicab would generate mistrust among the parties of the system. Specifically, if the statistics about taxicab quality service affects the decision to renew a taxicab licence or even worse, a notice of a revocation of the licence. Therefore, the process 6 en-
7. Security Analysis 101

Ensures the taxicab has been authenticated by the user by means of a temporal ID, a fare issued by the taxicab driver and a signature emits by the TAXI Fare application.

7.2.4 Falling to report incomes

Another advantage that the scheme implemented for taxicab companies is not to report all journeys made by the taxicab drivers. The statistics, generated by the process 7, can be modified to include an additional field, the taxi fare issued by the driver. Then, no journeys can be denied by drivers and owners can be guaranteed all incomes from taxicab operation are taken into account and enhanced.

7.3 Summary

In the section 5.1, it was described how every requirement is successfully achieved by one or more processes. However, it is important to emphasise the responsibilities of users:

- Always keep his or her NFC-enabled device close to them and fully charged.
- Install an antivirus application and up-to-dates the patches of the Operating System of the device.
- Keep connect the device to the Internet to receive the up-to-dates of the revoked taxicab and valid Licence Operators certificates.
- Always get into a taxicab using the door where is the contactless smart card placed on.
- Always verify the Licence number which appears on the screen is the same that is on the side-door of the taxicab.

In other parts of the Chapter were presented the main attacks concerning the users of the taxi service and how the TAXI scheme strives to mitigate them. However, criminals are always making new forms to get advantage of ordinary persons and local authorities might be appropriate to adjust the TAXI scheme to face new challenges, for example, modifying the maximum time required for the execution of the TAXI Authentication protocol (Process 5a) to avoid replay attacks.
8. CONCLUSIONS

In this report we highlighted the significance of the taxicab industry for three main sectors of the economy and, furthermore, to what extent could some changes in labour and taxi regulations be detrimental to the perception of safety by taxicab passengers leading to a reduction in the number of journeys and an economic downturn in several industries.

We considered the lack of effectiveness of current applications for giving security to the passengers when they hire a taxi in the street. Taking into account the taxicab regulation schemes and the issues concerning their passengers as a starting point, we set three groups of security requirements: User safety, Quality service and system’s capabilities and efficiency.

The novel TAXI Authentication scheme was created as a response to the need to address those requirements. It is based on the increasingly accepted NFC technology and the tamper-resistant smart cards to construct Front-office processes, particularly noteworthy is the TAXI Authentication protocol designed as a modified DDA authentication protocol for efficiency and scalability reasons due to the main drawback of symmetric authentication methods to consume an excessive amount of resources such as network bandwidth and processing at the back-office system.

The quality service feedback that preserves the anonymity of users facilitating the quality assessment. Whereas, a robust Key Management System supports the Back-office processes grounded in certificates using ECDSA digital signatures due to its efficient performance in smart cards and short-length keys providing a high level of security.

We conducted the preliminary security analyst against the proposed security requirements. After that, we applied to real world criminal use-cases concerning the taxicab passengers. The scheme shows promise of combating potential crime under whichever type of taxicab regulation scheme demonstrating great flexibility to adapt to a great number of circumstances and future attacks against the industry.
8. Conclusions

8.1 Further work

For improvement of this project, as a first step, an implementation of a pilot project in a small-size city can be done in order to make corrections to the TAXI Authentication scheme finalising details in the design and develop the components of the scheme adjusting parameters according to the needs of the case.

With regard to improving the design of the scheme. The TAXI Local Authority subsystem is the component of the scheme with more roles and responsibilities in the processes. Then, it was made a high-level description of the four modules which component it in order to envisage the possibility of third parties become involved in the scheme to reduce the workload pressure on the Local Authorities.

The licences for drivers were not included in the TAXI scheme so as not to adversely affect the flexibility required in order to the scheme can be adopted by whichever taxicab regulation industry. Nevertheless, the licences would be implemented as a new type of certificates in the hierarchy and they might be generated by the TAXI Licence Operator subsystem and include into the TAXI Fare application as a new application in the active NFC tag thanks to the tag stores an internal clock to verify the date and time of shifts of every driver whom can possess an NFC-enable device for authentication.

The option to include a remote installation of the TAXI Mobile application in the SIM card of mobile phones using Over-The-Air (OTA) technology by the MNO (Mobile Network Operators) should be approached with caution in order to not exclude other mobile NFC-capable devices which no possess a SIM card such as PDA, tablet computers, netbooks, and portable video game consoles, specially when those are connecting to the Internet using WiMAX technology.

The TAXI Mobile application and the administration of the user module in the TAXI Local Authority subsystem might include further control to corroborate that all users have received the up-to-dates of certificates and the latest version of the application.
BIBLIOGRAPHY


[34] London Chamber of Commerce and Industry, “The london taxi trade.”

   2012.


[37] L. Commission., “Reforming the law of taxi and private hire services,”

[38] A. Marell., “The effects of taxicab deregulation in rural areas of sweden,”


[40] M. R. Sweeney., “United states v. woodrum, beware taxicab passen-

   http://www.london.gov.uk/mayor-assembly/london-assembly/


   tfl/gettingaround/taxisandminicabs/taxis/default.aspx. Ac-
   cessed: 2014/02/11.


