Nicolás Villalobos Ramírez

Lightweight cryptography for multimodal transportation of citizens

Master's Degree Final Project

Directed by Dr. Antoni Martínez-Ballesté

Master's in Computer Security Engineering and Artificial Intelligence

UNIVERSITAT
ROVIRA i VIRGILI

Tarragona

2022

Abstract

This master thesis examines current research and advancements in the security controls and cryptography techniques applied to ticketing systems deployed in multimodal transportation services. The focus is put on understanding the security safeguards protecting contactless smartcards and smart devices as fare payment means to access public transport services. To this effect, both proprietary and open ticketing schemes are reviewed such as MIFARE technology and Calypso standard, respectively.

Our review also includes understanding the implementation of smart ticketing technology in smart cities that counts with a central fare system that grants access to all public transport services through a single smart device such as smartcards, smartphones, or wearables. These smart cities include Paris, London, Hong Kong, Tokyo, Singapore, Sydney, Madrid, and New York City.

Finally, potential security attacks that these systems might be susceptible to are also explored outlining the implications a successful one might have when it comes to compromising the underlying infrastructure as well as impacting the privacy of passengers.

Keywords: contactless, smartcard, NFC, cryptography, security, public transport, privacy, railway, smart transportation.

Resumen

Este trabajo de fin de master examina los avances e investigaciones actuales sobre los controles de seguridad y técnicas criptográficas aplicadas a sistemas de ticketing desplegados en servicios de transporte multimodales. El interés es entender las medidas de seguridad implementadas durante el uso de tarjetas contactless y dispositivos inteligentes para el pago de tarifas en el transporte público. A este efecto se revisan sistemas de ticketing propietarios y públicos como por ejemplo la tecnología MIFARE y el estándar Calypso.

Nuestra revisión también incluye entender la implementación de la tecnología detrás de los sistemas de ticketing inteligentes instalados en ciudades inteligentes que disponen de un sistema de tarifas central para acceder a los transportes públicos a través de dispositivos inteligentes, ya sean una tarjeta, teléfono móvil, o wearable. Estas ciudades inteligentes incluyen Paris, Tokio, Madrid, Sídney, Londres, Singapur, y Nueva York.

Finalmente, se estudian los potenciales ataques de seguridad a los que estos sistemas pueden ser susceptibles a la vez que se exploran las implicaciones que tendría un ataque exitoso que comprometa la infraestructura subyacente, así como su impacto en la privacidad de los viajeros.

Palabras Clave: contactless, tarjetas inteligentes, NFC, criptografía, seguridad, transporte público, privacidad, transporte inteligente.

Contents

Figures

Acknowledgements

To my parents and friends for all their support and encouragement throughout the years.

Abbreviations

3DES: Triple Data Encryption Standard

AES: Advanced Encryption Standard

AWS: Amazon Web Services

BAU: Business As Usual

CAC: Common Access Card

CIA: Confidentiality, Integrity, and Availability

CPU: Central Processing Unit

CRTM: Consorcio Regional Transporte Madrid

DES: Data Encryption Standard

DoD: Department of Defense

DDoS: Distributed Denial of Service

DHE: Diffie-Hellman Ephemeral

ECDHE: Elliptic-curve Diffie–Hellman Ephemeral

DoS: Denial of Service

ECC: Elliptical Curve Cryptography

EEPROM: Electrically Erasable Programmable Read-Only Memory

GE: Gate Evaluation

HCE: Host Card Emulation

I/O: input/output

IC: Integrated Circuit

IoT: Internet of Things

IV: Initialization Vector

ISO: International Organization for Standardization

ITSO: Integrated Transport Smartcard Organization

LWC: Lightweight Cryptography

NDA: Non-Disclosure Agreement

NFC: Near Field Communication

NIST: National Institute of Standards and Technology

MFA: Multi Factor Authentication

MITM: Man-in-the-Middle

PII: Personally Identifiable Information

POS: Point of Sale

RAM: Random Access Memory

RFID: Radio Frequency Identification

ROM: Read-Only Memory

RSA: Rivest–Shamir–Adleman

SE: Secure Element

SSL: Secure Sockets Layer

TfL: Transport for London

TLS: Transport Layer Security

WAF: Web Application Firewall

WoS: Web of Science

Chapter 1: Introduction

This chapter covers the reasons and motivation behind making security and privacy in public transportation services the core of the thesis. A high-level overview of the content as well as the structure of this document is also covered.

1.1) Motivation

In this fast-paced society, thousands of workers commute every day to workplaces located in big metropolitan areas and their surroundings. Commuters heavily rely on private cars or other private means such as company-provided buses or carpooling when workplaces are not easily accessible by public transportation.

This commuting in and out of cities impacts the overall traffic flow thus introducing road congestion issues caused by the major presence of privately owned vehicles. This not only impacts the traffic in cities but also introduces additional pollution and raises environmental concerns.

City governments often implement policies that attempt to tackle this by minimizing the presence of private vehicles circulating in metropolitan areas whilst enhancing the features and presence of public transportation. These policies could take the form of additional taxes or fees to circulate the city or discounted public transportation fares, among other initiatives. Detailed planning and a reliable and efficient mass transportation system are essential to cover the transportation needs of citizens to achieve the goal of seamlessly moving millions of people throughout cities.

In the context of smart modern cities, different transportation means coexists. From the more traditional ones such as trains, buses, and metro to more modern alternatives such as car-sharing apps, temporary bike riding, and temporary rental of electric vehicles. An essential point to encourage the use of these services is the seamless access to them all by using a single payment system.

Traditionally, each transport means has been operated by different companies thus having different fare payment systems. In these situations, passengers must carry all their seasonal passes if they want to access public transportation services without paying for a single trip ticket. Modern smart transportation considers the simplification of fare systems into one single system that interconnects the different transportation services available within a city.

These fare collection systems play a key role in granting access to public transport as users must present a valid pass or ticket to use the service. Modern ticketing systems involve the use of contactless smartcards to access transportation services, which helps in reducing unpleasant delays as passengers do not need to fiddle with coins or cash. This is not the only advantage of these systems as they are also capable of collecting a great amount of data. This data, however, is a double-edged blade as on one hand transport authorities can benefit from it to better understand passenger needs, adjust timetables, expand, or reduce a certain route, and so on. On the other hand, the amount of data collected can raise concerns about users' privacy.

Therefore, security must play an essential component in these systems to ensure that both data and users are protected, whilst respecting their privacy.

1.2) Research Contribution & Objectives

The objectives of this master's thesis are to understand the current cryptographic techniques used in multimodal transportation implemented in cities to envisage best practices that ensure the security of both data and passengers. To achieve this, the following work is considered:

- Study the different use cases and electronic methods involved in multimodal transportation (i.e., user identification, smart ticketing systems, smartphone apps, etc.)
- Search and review real-world examples of integration of different transportation means within the context of a smart metropolitan area
- Understand off-the-shelf lightweight cryptography techniques that could be used in multimodal transportation
- Best practices and recommendations for a secure, privacy-enhanced multimodal transportation system, from different perspectives: devices, infrastructure, and protocols.

1.3) Structure

The structure of this master's thesis is as follows:

- **Chapter 2: concepts.**
  This chapter includes information about relevant concepts used in this work.

- **Chapter 3: literature review.**
  It contains details about the methodology used to search for papers, documents, and information relevant to this work, as well as an analysis of the selected ones.

- **Chapter 4: standards and technology.**
  This chapter includes information about the international standards that regulate the specifications of smartcards. Both proprietary and open technology and schemes are also described.

- **Chapter 5: real-world examples.**
  It is dedicated to the analysis of real-world multimodal systems used. This includes details about how they work alongside the protocol and cryptography techniques used to guarantee the privacy of public transport users should this info be available.

- **Chapter 6: Madrid Public Transport Analysis.**
  Analysis of the technology implemented in Madrid's public transportation system covering buses, metro, and commuter trains.

- **Chapter 7: cryptograhic protocols**.
  Cryptograhic algorithms found in the ticketing schemes reviewed alongside relevant lightweight ciphers in the context of smart cities and transportation.

- **Chapter 8: conclusions and future work.**
  Includes the conclusions of this work and proposes different ways to conduct further investigation on this topic.

Chapter 2: Concepts

2.1) Internet of Things (IoT)

The term Internet of Things (IoT) was coined in 1999 (1) and could be defined as the interconnection of physical objects with sensors, software, and other technology that exchange data and interact with other systems over the Internet or private networks (2).

These physical objects can be found in a wide variety of industries such as fashion, appliances, automotive, housing, wellbeing, etc. Just to name a few examples: fridges, clothes, watches, vehicles, light bulbs, smart homes, etc.

Public transportation is another sector, no stranger to IoT as interconnected devices are needed to improve the quality of service. Thanks to sensors integrated into public transport vehicles, it is possible to track their location, calculate the estimated time to arrive at certain stations, monitor the number of passengers, fuel consumption and much more. (1) This will, in turn, translate into higher user satisfaction, reduced delays for passengers, more efficient routes, and less overall pollution and noise.

For instance, the public transport company in Copenhagen, Movia, tested a pilot IoT project to detect whether buses were empty or full based on sensors deployed on them to count the number of mobile phones with internet connectivity. This was done in response to the novel COVID-19 pandemic to inform passengers, waiting at a bus stop, whether the incoming bus is full or empty as full buses are not meant to pick up any new passengers. (1)

As with any other device connected to the Internet, cybersecurity concerns arise, and effective countermeasures must be developed to protect them against malicious third parties.

Several attacks powered by compromised IoT devices have been carried out. For instance, one of the largest DDoS attacks, the Dyn attack, was caused by the Mirai Botnet through using millions of compromised IoT devices. Once a device was infected by Mirai, the malware would actively seek other vulnerable IoT devices with default credentials. The attack resulted in huge portions of the internet being inaccessible to legitimate users. (3) (4)

Another example that outlines why security on IoT devices is important is the Ring case in which thousands of Ring cameras were compromised. In this attack, threat actors were able to invade the privacy of Ring's customers by connecting to their in-home cameras to observe their movements, listen to them, and even interact with them (5)

2.2) Modes of transport

Modes of transport or modes of transportation refer to the different ways in which people and freight can be transported from one place to another (6). These ways are grouped into the categories of Land, Air, and Water. Three other transportation modes will also be mentioned here, which even though will not be relevant to this present work, are also included for completeness. These are:

- Pipelines: to transport gas & oil
- Cable: internet, energy supply
- Space: satellite telecommunications

Each mode of transport has its means of transport (7), which refers to the facilities used to transport cargo or people depending on the chosen mode. For instance, for transportation over land, means of transport could be cars, vans, buses, bikes, e-scooters, trains, etc.

Depending on whether a single or combination of modes of transport is used for a single trip, we talk about unimodal, intermodal, and multimodal transport. Unimodal transport is understood as the transportation of goods and/or people by a unique mode of transport during the entire route. The route could be over roads, railways, sea, air, etc. It is important to note that to be considered unimodal transport, the same mode of transportation must be used throughout a single trip. (8)

Similarly, this concept can also be extrapolated to the transportation of people. In this case, unimodal transport refers to the use of only one transport mode on a single trip for one trip purpose (9). For instance, this could be taking a single bus route to your destination.

Multimodal transport, also known as combined transport, refers to the transportation of goods or people by at least two different modes of transport on a single trip. In the transportation of citizens, multi-modal systems refer to passengers being able to enjoy a diverse range of transportations to get from A to B. This could be a city whose transportation services include metro, train, bus, taxi, eScooters, ride-sharing apps, ferry etc. However, we often find its implementation as a segmented system with different fares and ticketing systems for the different providers involved. (10). To simplify this, the development of a system that integrates fare payments is needed.

2.3) Smartcards

Smartcards are card-like devices with built-in microprocessors and integrated circuits. They interact with their environment through a chip embedded in the card, contactless technology through NFC, or both depending on the model. They have a rectangular shape with a dimension like regular bank cards, and they are mostly made from plastic.

2.3.1) Smartcard Architecture

The general architecture of smartcards is composed of three main elements, the I/O system, the CPU, and memory. The I/O (input/output) system is formed by the specific components that allow the card to interact with its environment. For contactless smartcards, the antenna lets the card communicate with a terminal through radio waves. Other smartcards such as bank cards also have a chip for contact interaction whereby the card is physically inserted into a terminal.

The CPU or microprocessor processes and stores information and can also be used for the authentication of users. The microprocessor is connected to both the I/O for handling communication and to the memory section of the card.

Memory is broken down into ROM (Read-Only Memory), RAM (Random Access Memory), and EEPROM (Electrically Erasable Programmable Read-Only Memory). RAM is used for fast computation and response. Its content is erased when no power is supplied. ROM is where the Operative System (OS) or runtime environment is located whereas EEPROM serves as persistent storage for data. (11)

Figure 1 shows the building blocks that compose a smartcard for an easier and clearer understanding of the components as well as the interaction among them all. The Co-CPU is an additional microprocessor that assists the main CPU in computation tasks, for instance, this can be a cryptoprocessor that handles all cryptographic computation.

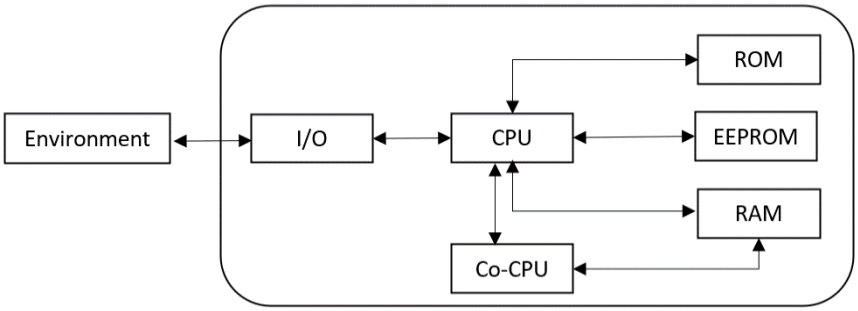


Figure 1. Smartcard Overall Architecture

2.3.2) Mobile payments

It is not strange anymore to see customers simply tapping their smart devices to pay at a grocery store, cafeteria, or their favourite retailer. Customers simply need to hold them in proximity to a point of sale (POS) terminal to validate the sale and perform the monetary transaction. It is easier, convenient, and simple for users.

This is possible thanks to a technology standard called Host Card Emulation (HCE) which allows to effectively emulate a physical bank card on software. Users no

longer need to carry a physical card around; they only need their phone or a smart wearable device such as a smartwatch.

HCE works via a Near Field Communication (NFC) chip embedded within compatible devices. When a user holds its device close to a POS terminal, the device communicates with the bank's server through mobile networks to validate the authenticity and process the transaction.

Before HCE there was another solution that leveraged NFC technology, this is the Secure Element (SE). When it came to mobile payments, the SE chip would be hosted internally in the device to allow communication between it and the reader.

There are two main differences between SE and HCE, SE is located within the device whereas HCE is on Cloud; Telecom providers and smartphone manufacturers could control access to the SE chip, thus limiting what systems it can interact with. With HCE there is a change in the paradigm as it is no longer a service used for mobile, but it is open to integration with other applications such as storing transport passes and holding multiple cards and wallets. This change to HCE is transparent to both merchants and users as HCE supports the current POS terminal with NFC capabilities. (12)

From Android 4.4 onwards, Google introduced HCE compatibility to avoid relying on the SE. In this way, any Android application could emulate a card and simply communicate directly to the reader without relying on the third-party SE.

Google Dev portal explains the differences between using an SE and HCE. When SE is used, the emulated card is stored in the SE through the app. At a POS terminal, the NFC controller routes all data from the POS reader to the secure element as shown in the image below:

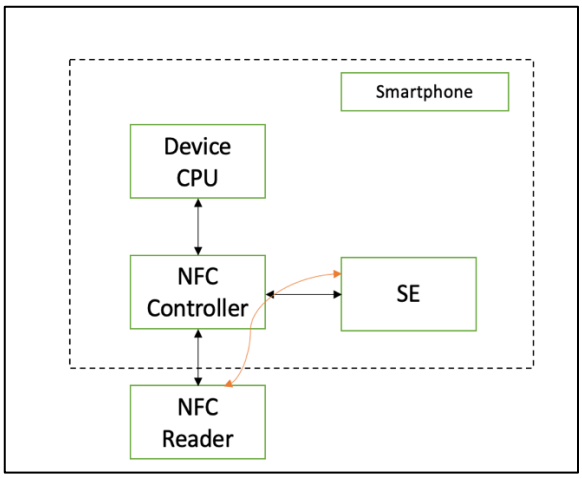


Figure 2. NFC card emulation with SE

As can be seen, the communication flow occurs purely between the SE and the NFC reader. No application is involved in this transaction.

On the other hand, when HCE is used to emulate a card, the data flow occurs directly between the NFC reader and the Host CPU. One of the advantages of HCE is that the service runs in the background without needing to open an app to interact with a POS terminal. The idea is that when the communications are initiated between the reader and the smartphone, Android selects the right service. (13)

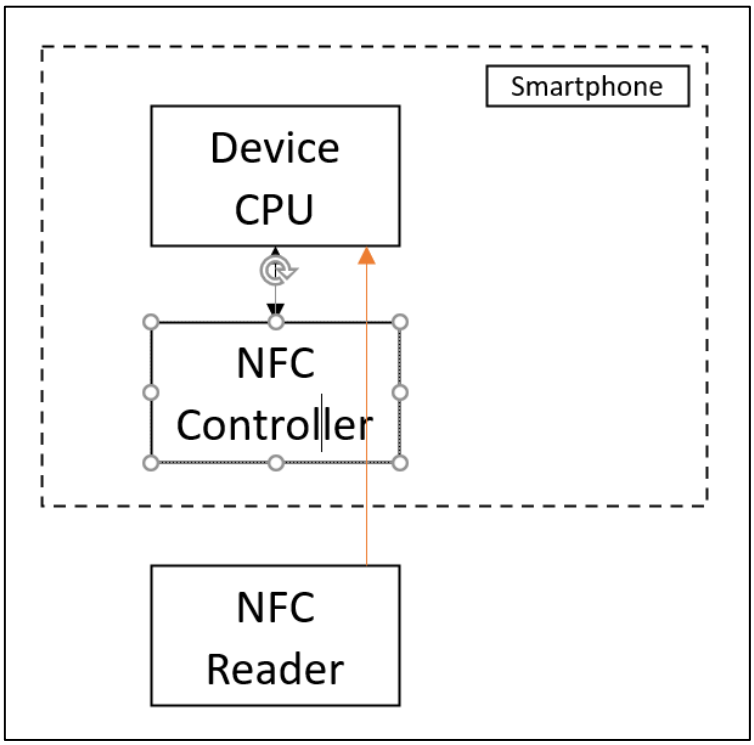


Figure 3. NFC card emulation without a Secure Element

2.3.3) Smartcard Applications

Smartcards can be found in different sectors and applications such as the following:

Healthcare

Smartcards in healthcare can assist patients and hospitals alike in different ways such as proving patients' identity, accessing patients' medical records, reducing the incidence of medical identity theft, and many more. It provides a secure mean to carry private medical information from one healthcare provider to another.

For instance, it can be used by first responders to access the clinical history to check for any allergies, pathologies, or previous injuries on their way to the hospital when patients are unconscious, injured, or too confused to inform doctors about historic health conditions.

Figures 4 and 5 below show examples of smartcards used in healthcare. The former depicts a smartcard sample in the United States whereas the latter presents the smartcard issued by the Andalusian government to access medical care services in the Andalucia region, Spain. As can be seen, both are similar in terms of appearance with

the main difference of the latter not including a photograph of the card owner. However, they both have a chip that carries health information and identify the user.

Figure 4. Healthcare Smart Card Example (14)

Figure 5. Smart Medical Card in Andalucia, Spain

Banking & Finance

In the banking & finance sector, smartcards refer to regular bank cards, either debit or credit ones. Traditionally, bank cards would have to be swiped through a POS so the data embedded in the magnetic strip could be read. User identification occurred through that data and needed customers to sign a receipt and show a national ID as evidence of identity.

Later, chips were introduced so that users would only need to insert the card with the chip facing the terminal and enter a secret PIN code only known to the user. The latest addition to bank cards is contactless NFC functionally so that users could simply tap the card on the reader. However, contactless does not entirely remove the PIN feature as should the user spend above a certain threshold, the POS would prompt the user to enter the PIN.

Figure 6 below shows an example of a bank card, in this case, a debit card issued by the HSBC bank.

Figure 6. HSBC Debit Smart Card (15)

Government resources

Smartcards are also used to grant access to government resources and areas by assisting in the identification of users. In the United States, the Department of Defense (DoD) counts with one of the most advanced smartcards called Common Access Card (CAC).

The card serves as a standard to identify active military personnel, civilian employees, and contractors. It also grants access to computer networks and systems. (16)

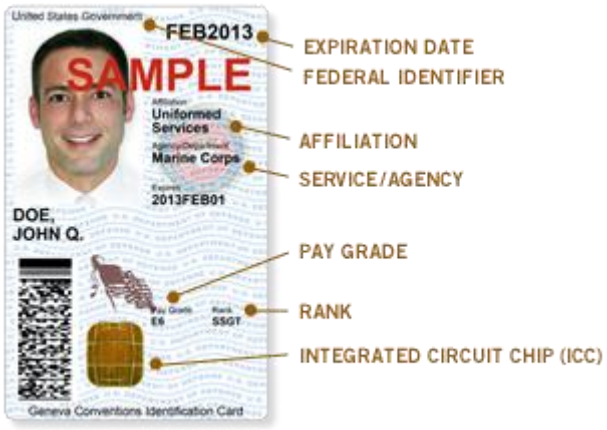


Figure 7. Common Access Card (CAC) (16)

Educational systems

Smartcards are used in educational systems to identify students and grant access to resources, services and/or areas within schools or universities such as paying for a meal in the canteen using meal credits, accessing printer services or withdrawing a book from the library.

Figure 8 Smart Student Card (17)

Public Transportation systems

In the context of public transportation systems, smartcards are used to grant access to buses, metro, subways, trams, or trains by allowing passengers to pay the service fare through them.

Figure 9. Smartcard Compass used in Vancouver (18)

Depending on their implementation, these cards can serve as a wallet that contains a monetary value that decreases each time transport services are used or can hold a specific number of journeys or allow journeys for a specific time window (daily, weekly, monthly, and yearly).

Smartcards are being rolled out globally to simplify access to mass transit services. Hong Kong, the United Kingdom, and Japan have successfully deployed schemes based on smartcards with contactless functionality called Octopus, Oyster, and Suica respectively.

Figure 10 shows a non-personal version of the Renfe & Tú card that allows passengers to access commuter train services throughout the Renfe railway network in Spain. Concerning its technology, they count with a small chip and an RFID antenna to allow the contactless mechanism. The chip is based on MIFARE Plus SE technology (19)

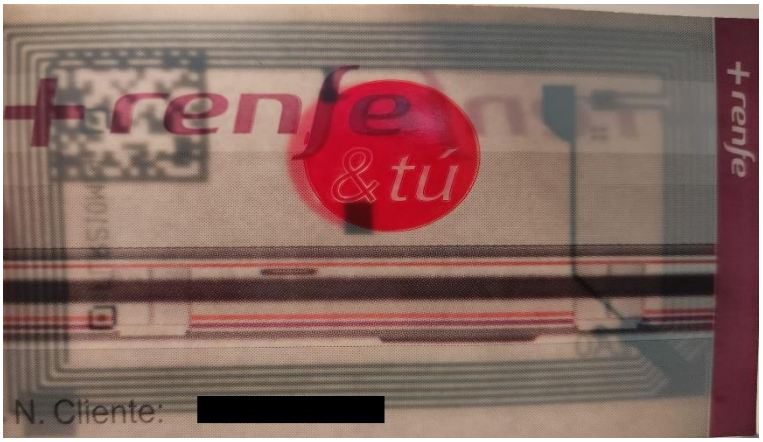


Figure 10. Renfe & tú non-customized smart card

As can be seen in the figure, the RFID antenna is visible by holding the card against a strong light. The card itself does not include any printed details of the user, so it is completely anonymous. No national ID or passport must be presented to obtain one of these as they are available in vending machines at train stations.

Each of them counts with a client ID number that is simply used to accumulate points and enjoy discounts later. However, it does not identify the holder. On the other hand, there exists a personalized version of the card that contains information about the holder such as name and surname alongside a picture.

2.4) Smart Ticketing Systems

Ticketing systems oversee the expedition of tickets and pass to access transportation means. The traditional ticket is a piece of paper printed by a vending machine at a train station, a bus station, or directly from the station staff, including origin and destination.

In the traditional payment system, tickets were paid in cash thus incrementing the probability of delays as passengers would need to fiddle with coins to pay the exact fare. Imagine a bus waiting at a stop, people lining up to onboard it, opening their wallet/purse, locating the right coins, and then the driver counting them and printing the ticket.

Ticketing systems have evolved to include more alternatives to access transportation services. Users can now buy tickets in advance through websites and smartphone apps and then import them into digital wallets or print them. These tickets often include a QR code which users simply scan to access transport services such as Renfe railway in Spain of First Bus buses in the UK. Another innovation to these systems is contactless functionality powered by NFC which allows fare payment by tapping a transport smartcard and a debit or credit card either physically or stored in smart devices.

Apart from the benefit to the environment introduced by removing the need for printing tickets, new technology alternatives provide convenience, ease to passengers, and interoperability. (20)

2.5) Cryptography

Cryptography refers to the area of study of developing techniques and mechanisms to secure communications in a way that only the sender and the intended recipient can view a message.

This is achieved by leveraging encryption algorithms to transform a given input, called plaintext data, into an encrypted output called ciphertext. The opposite process is called decryption in which a given ciphertext is transformed into its original plaintext. (21)

Encryption assists in protecting the confidentiality of data. Confidentiality refers to protecting sensitive information from unauthorized parties whilst implementing the relevant safeguards to make the data available to authorized personnel.

Confidentiality is part of the cybersecurity CIA triad, being the other two Integrity and Availability. Integrity refers to controls that protect against the unauthorized deletion or modification of data, and Availability ensures that information is available anytime an authorized individual requests it. (22)

Two types of cryptography exist depending on whether the same key is used for the encryption and decryption process, or different keys are used. These are called symmetric and asymmetric key encryption algorithms, respectively.

2.5.1) Symmetric key encryption algorithm

Symmetric key encryption algorithm refers to ciphers that use the same key to perform both encryption and decryption operations. Their implementation takes two forms in the way of block ciphers or stream ciphers. The former encrypts blocks of plaintext with a specific size whereas the latter encrypts individual digits.

Using the classical example of Alice and Bob, Alice has a message (M) that wants to send to Bob. She does not want anyone else but Bob to access the message. Therefore, Alice leverages encryptions and uses a key (K) to encrypt the message. The encrypted message (M') is sent to Bob who uses the key (K) to decrypt and get the original message (M). Bob can now read Alice's message.

Some examples of symmetric key ciphers are:

- Data Encryption Standard (DES)
- Triple-DES (3DES)
- Advanced Encryption Standard (AES)
- Blowfish
- Salsa20
- ChaCha20

2.5.2) Asymmetric key encryption algorithms

Asymmetric key encryption algorithms, also known as Public-key cryptography, use two different keys to perform encryption and decryption operations. These keys are called public keys and private keys. In this type of ciphers, the public key is used for encryption and the private one is used for decryption. (21)

Within its applications, we find encryption data in transit, for instance, between a website and a client. When a client navigates to a website that supports HTTPS and has a valid TLS/SSL certificate, the web browser derives the public key of the certificate and uses it to encrypt the data. The website is the only one that can decrypt it by using its private key.

The most relevant asymmetric key algorithms are (23):

- Diffie-Hellman
- RSA
- DSA
- Elliptical Curve Cryptography (ECC)
- ElGamal

2.5.3) Encryption at rest & in transit

There exist several cryptography techniques to protect the confidentiality of the information and they could be divided into encryption at rest and encryption in transit.

Encryption at rest refers to applying cryptography algorithms to protect information stored. Symmetric key algorithms are preferred for this type of protection due to their performance. On the contrary, encryption in transit refers to applying ciphers that protect information on the go like moving information from one server to another. Asymmetric-key ciphers are suitable for encryption in transit.

2.5.4) Lightweight cryptography (LWC)

Traditional cryptographic algorithms were designed for desktop and server environments where processing power and energy consumption were not a concern. With the rise of the IoT and embedded systems, the necessity arises to explore cryptographic algorithms that are lighter in terms of space, needed resources, power and energy consumption. IoT devices are mainly small which limits the capabilities in terms of batteries, computational power, etc. Hence, it is fundamental to apply encryption algorithms that require low computational power.

Traditional algorithms no longer apply to constrained devices as they consume too much energy, too much processing power, or simply too much physical space for storage (24). Even in the case of current algorithms are managed to run in constrained devices, their performance might not be acceptable (25). Therefore, a solution to provide security and privacy to these devices needs to be explored.

One of the techniques that aim to overcome this problem is lightweight cryptography (LWC). Lightweight cryptography can be thought of as a subfield of cryptography that aims to explore cryptographic solutions suitable for constrained devices (26). These solutions feature a small footprint and low computational complexity. These constrained devices include RFID tags, contactless smartcards, sensors, embedded systems, IoT, etc (27).

According to (28), there are two different ways to obtain the lightweightness of a certain cryptographic cipher: optimizing the implementation depending on constraints or generating a specific design that considers smaller internal states, key sizes, etc. The lightweightness of a given cryptographic algorithm can be measured in terms of the following metrics:

- Power and energy consumption
  This is important for battery-powered devices

- Latency
  How long it takes to perform a certain task. Important to devices where a fast response is needed.

- Throughput
  It is measured in Bps (bits per unit). Measures the rate the plaintext is processed by the algorithm.

- Resource requirement
  Based on whether it is a hardware or software implementation. Hardware implementation works better for highly constrained devices whereas software implementation is better suited for less constrained devices.

As with regular symmetric encryption algorithms, lightweight ones can be further divided into block and stream ciphers. Some relevant stream ciphers are Espresso, Trivium, Chacha, and WG-8.

Chapter 3: Literature review

The focus of this literature review is to identify papers that discuss the application of cryptographic techniques to mass transportation services, especially around smartcards technology and ticketing systems.

We aim to select publications relevant to this master thesis to support the ideas behind it and explore techniques in use to protect ticketing infrastructure and understand the attack vectors that could threaten mass transit services and passengers' privacy. In special, we aim to provide answers to the following questions:

1) Smartcard security mechanisms and vulnerabilities
2) Ticketing systems security and vulnerabilities
3) Privacy concerns in public transportation

3.1) Search methodology

In our literature search, we have looked for articles, papers, reports, conference proceedings, and research works relevant to the topic at hand. To conduct this search, we mainly focused on two scientific databases: Web of Science Core collection Database (WoS) and IEEE.

We have followed a two-phased review methodology whereby we first attempt to identify a potential list of relevant works, which are then screened to select the ones that fit the most. To select the papers, we first reviewed the abstract and title and had a brief view of the document. If the content matched the purpose of this work and was thought would add value, it was then selected for further review and analysis.

Searches were performed on 10th April 2022 using the WoS Core collection database. To maintain consistency, we decided to remove publications not written in English as well as duplicates. Another important factor to consider is the number of citations as they are a good indicator of the quality, performance, and impact of a publication (29). Normally, over 100 citations are recommended. However, most recent papers might be left behind as they might not have yet reached the number of required citations.

The first area we covered was the security mechanisms used to protect smartcards. For this we used the following search string on WoS using the core collection database:

S1= ((ALL=(card)) AND ALL=(security)) AND TI=(survey)

The *All* field performs a search over all the searchable fields whereas the *TI* one only searches the given keyword over the publications' title. As we are interested in finding recent surveys, we limited the search to publications released within the last 5 years. The search yielded a total of 23 publications.

To select the most relevant ones, we first sorted the results based on their number of citations from highest to lowest, and then, their abstracts and titles were reviewed. Publications that were found suitable were then fully reviewed if the full paper was available, otherwise, it was discarded. From this search, we found 5 relevant papers although only access to three of them was available.

In addition to this search, we also performed another one on IEEE Xplore using the following query string:

S1' = ("All Metadata":smartcard OR "All Metadata":smart card) AND "Document Title":security

All Metadata field performs a search of the given keyword over the paper's metadata. *Document Title* searches over the paper's title. In this case, as the query was slightly different to the one performed on WoS, we decided to expand the timespan and filter publications published from 2007 onwards. This query yielded 287 results.

Following the same procedure, the publications were first sorted by the number of citations and then initially reviewed by inspecting the title and abstract. This inspection yielded a list of 5 candidates for further examination.

Our second area of interest was to understand which safeguards are used to protect ticketing infrastructure. To achieve this, we again relied on the WoS Core Database collection and performed a search using the following query string:

S2 = (TS={"security"}) AND (ALL={"transport" & "ticketing"})

The *TS* field performs a search over a topic through a given keyboard. This yielded a total of 92 publications. No timespan was chosen for this query. After reviewing the title of the available publications, 18 were found suitable. We then delved into the abstract to further assess its suitability, which yielded 3 suitable papers for close examination as one of them was duplicated.

We were also interested in searching for particular security concerns on buses, metro, and train transport means. To this effect, we conducted another search using the next query string:

S2' = (TS={"transport"}) AND (ALL={"security"}) AND (TI={"bus" OR "train" OR "metro"})

This yielded 144 publications of which only 3 of them were suitable after inspecting the title and abstract.

Moving on to the next sets of publications, we aimed to check privacy concerns that arise in public transportation. Again, we relied on WoS Core Database collection and conducted the following search:

S3 = ((ALL={"ticket"}) AND (TI={"privacy"})

The query resulted in a total of 66 publications of which only 7 were considered potential candidates. In the end, only 5 were found suitable and as such, were selected.

Table1 below shows the number of publications at each step of the review process:

Table 1. Publications considered at each step of the process

Set	Potential Results	Potential results after the review	Final selected publications
S1	23	5	3
S1’	287	5	5
S2	92	18	3
S2’	144	4	3
S3	66	7	5

3.2) Selected Papers

Table 2 below outlines the papers that were selected for further analysis during this work.

Table 2. List of selected papers

No.	Title	Year	Set
1	A Survey on Contactless Smart Cards and Payment System: Technologies, Policies, Attacks and Countermeasures	2020	S1
2	A Survey on Lightweight Authenticated Encryption and Challenges for Securing Industrial IoT	2019	S1
3	A Survey on Lightweight Cryptographic Algorithms	2018	S1
4	Host-based Card Emulation: development, security, and ecosystem impact analysis	2014	S1’
5	Lightweight Cipher Algorithms for Smart Cards Security: A Survey and Open Challenges	2017	S1’
6	Overview of Security Threats for Smart Cards in the Public Transport Industry	2008	S1’
7	Power Analysis Attack: A vulnerability to Smart Card Security	2015	S1’
8	Security Evaluation of Apple Pay at Point-of-Sale Terminals	2016	S1’
9	A survey of electronic ticketing applied to transport	2012	S2
11	Mobile Ticketing with NFC management for transport companies. Problems and solutions.	2013	S2

12	Privacy-Preserving Electronic Ticket Scheme with Attribute-Based Credentials	2019	S2
13	Smart Metro Rail Ticketing System	2019	S2’
14	Metro Automatic Fare Collection System Safety and Security	2017	S2’
15	Vulnerability analysis of urban rail transit based on complex network theory: a case study of Shanghai Metro	2017	S2’
16	Passengers information in public transport and privacy: Can anonymous tickets prevent tracking?	2014	S3
17	Privacy-Preserving Billing for e-Ticketing Systems in Public Transportation	2013	S3
18	Privacy-Preserving Public Transport Ticketing System	2015	S3
19	User Privacy in Transport Systems Based on RFID E-Tickets	2008	S3
20	A Privacy-Preserving Ticketing System	2008	S3

3.3) Literature analysis

Nowadays, cybersecurity and privacy concerns are of significant importance across all industries. Considering the rapid development and adoption of technology across sectors, public transportation infrastructure is of special interest as it is critical for the regular functioning of modern cities.

Mass transit authorities around the world have embraced technology developments to improve their services whilst reducing costs. Traditionally, two areas were of special interest, fare collection and service speed and reliability. Today, as security and privacy concerns arise globally and users are savvier and more conscious of their data, a third factor enters the equation, the safety and privacy of riders’ data.

In “*A survey of electronic ticketing applied to transport”* (30) the authors present the recommended security requirements of electronic tickets. These are:

Integrity

Tickets shall not be manipulated and its verification should be possible by all parties,

Unforgeability

Tickets can only be issued by authorized users or authorities.

Fairness

Passengers and transit authorities stand in a similar situation, and nobody is in a privileged one. If users paid for a service, they should receive it. If a user

presents a valid ticket, the service provider shall provide the service linked to that specific ticket.

Non-overspending

Not exploiting a way to use tickets further than their intended use, could be achieved by the use of tamper-resistant devices such as smartcards.

Portability

Tickets shall be portable.

Flexibility

Allow the use of tickets in different transport means within the same city.

Availability

The ticket shall be used when needed.

Since the implementation of smartcard technology, users can access services seamlessly and fast, however, a question arises concerning the security of their data. If communication between the smartcard and the transit authority's network is not properly secured, a malicious party could eavesdrop the communication and gain unauthorized access.

As we have previously mentioned, smartcards communicate through NFC technology. NFC is not exempt from attack vectors such as eavesdropping, skimming, and relay attacks (31). The first one affects all wireless communication as the message is transmitted over an insecure channel where malicious entities could be listening. It is claimed that these messages could be intercepted by a powerful antenna (32). The recommended safeguard against this attack is the use of encryption.

Skimming attacks are possible when the contactless card interacts with an NFC active device to copy the information available from the card. This information is then copied into another card, thus cloning it. The safeguard against skimming attack is access controls, thus info stored in the card is only accessible by the right devices. This data can also be intercepted during transmission, hence enabling unauthorized manipulation (33)

To protect NFC communication between the reader and smartcards, cryptographic ciphers such as DES, 3DES, AES, ECC, and RSA are used (34) (35). In the proceeding "*All about encryption in smart card*", the authors compared the efficiency of different asymmetric and symmetric ciphers on smartcards. They concluded that for encryption in transit ECC is more suitable than RSA due to smaller key sizes, faster computation times, and lower power consumption. Concerning encryption at rest, they compared DES, 3DES, and AES and concluded that the algorithm would depend on the criticality of the system, should security be the top priority, AES should be the go-to, but DES or 3DES should be selected is speed is more important (34). Similar research was conducted by M. Zhao in the paper "*Research on*

Encryption Technology on contactless IC Card" (36) to show that DES and 3DES ciphers are the most widely used in contactless technology.

A comparative study performed in the work "*Lightweight security algorithm for low power IoT devices*" (37) among Diffie-Hellman, Elliptic Curve Diffie-Hellman (ECDH), and Rivest, Shamir, & Adleman (RSA) showed that ECDH performs better in terms of power and area.

In "*A Survey on Symmetric Key Encryption Algorithms*." (38) The authors compared both symmetric and asymmetric ciphers for smartcard applications. They concurred that AES, 3DES, and Blowfish are more efficient in terms of less memory and area requirements as well as having more compatibility than RSA, and ECC. Blowfish has a key size varying from 32 to 448 bits, so it is effective in countering brute force attacks. The authors concluded that AES is better than others by the mean of providing security to both hardware and software implementation although the time taken by AES to perform encryption and decryption operations due to the key size adds constrain to smartcard devices.

In the paper "*A survey on Lightweight Cryptographic algorithms*" (39) the authors compare the performance of the most popular symmetric algorithms and compare them with lightweight ones. They claim that Blowfish stand out concerning its processing time even though it uses a long key of 448 bits. AES is faster and more efficient than DES, 3DES, and BlowFish. They also compared their power consumption on devices with restricted battery power and discovered that after around 600 encryptions of a 5MB file size with 3DES further encryptions are not possible as the battery dies. Therefore, highlighting the need for lightweight ciphers.

Concerning lightweight block ciphers, the authors compare algorithms such as ICEBERG, TEA, PRESENT, CLEFIA, and DES. ICEBERG uses 128-bit keys in 64-bit blocks through 16 rounds. It is fast and provides efficiency in encryption and decryption operations. (39)

DES is also investigated as a lightweight cipher although it presents the disadvantage of being less secure due to the smaller key size (56 bits). Therefore, further development was needed and some variants of DES were presented such as DESL, DESX, and DESXL. The first one requires around 50% less of the gates equivalent (GE) required to implement AES. The second one DESX is another variation used to fight against brute force attacks on the DES algorithm, it works by simply adding 8 bytes to the key size. In terms of hardware occupancy, DESX occupies 2629 GE. The last one, DESXL is a combination of DESL and DESX whose implementation only occupies 2169 GE (39).

TEA is another lightweight cipher using 128-bit keys with 64-bit blocks and 64 rounds. It was designed for power consumption efficiency and its security was enhanced by its extensions such as XTEA and XXTEA. The first one was introduced to address flaws when TEA was implemented with small rounds although the authors claimed that it introduced a block cipher named Block TEA that was weak. XXTEA was then

presented to amend this. XXTEA also uses 128-bit keys with 64-bit block and 64 rounds but in contrast to the original TEA, its implementation only requires a minimum of 2000 GE instead of the original 2100 (39).

PRESENT is considered a standardized block cipher for lightweight cryptography, pretty much like AES to traditional cryptography. It is an ultralight cipher capable of running on ultra-constrained devices with 1000GE for only encryption, and 1030 GE for both encryption and decryption operations (39).

CLEFIA is alongside PRESENT another standardized block cipher for lightweight cryptography. It was created by SONY and it can use a key size of 128, 192, and 256 bits through 18, 22, and 26 rounds respectively. Its most ultra-lightweight implementation occurs 2488 GE only encryption. If both operations are desired, the number of GE increases to 2604GE (39).

The authors then discarded ICEBERG as not efficient due to its implementation requiring 3000 GE. They mention that AES, PRESENT, CLEFIA, and DES variants are the most studied solution in the literature and therefore the most accepted ones (39).

The paper "*Current Lightweight Cryptography Protocols in Smart City IoT Networks: A Survey*" (40), mentions that traditional ciphers might not be suitable to protect IoT devices in modern smart cities due to scalability and the dynamic nature of smart cities. It is mentioned that lightweight algorithm block ciphers should have a smaller block size of 32-64 bits instead of the usual 64-128 bits.

Concerning AES, studies have been carried out to adapt it to IoT devices, hence, converting it to lightweight. In the paper "*Power efficient AES core for IoT constrained devices implemented in 130nm CMOS*", a power-efficient implementation called AES Core was presented for IoT constrained devices implemented in 130 nm technology (41). Another adaption of AES suitable for IoT was presented in the work "*A Compact, Lightweight and Low-Cost 8-Bit Datapath AES Circuit for IoT Applications in 28nm CMOS*" (42).

Smartcard vulnerabilities

As with any other technology, smartcards are not exempt from vulnerabilities. In the paper "*Overview of Security Threats for Smart Cards in the Public Transport Industry*" the authors explore the security concerns and threats of smartcards used in public transportation services. The attacks are categorized into physical, logical attack side channels, and rogue terminals (43).

Physical attacks aim to compromise a component of the smartcard itself such as the memory or the microprocessor. In this scenario, attackers need physical access to the card, therefore, the threat actors could range from the owner of the card itself to external entities that get hold of the card or even staff members. The authors claim that typical physical attacks involve attempting to read the memory of the card or using highly specialized and costly equipment to modify the architecture of the chip (43).

Logical attacks focus on compromising the regular operation of the card via exploiting weaknesses found in its operative system or application that make the card behave abnormally. To counter these types of attacks, the design and development process should include a security review process, which will likely catch most of the logical flaws.

Similar to logical attacks, side-channels attacks do not damage the card as they attempt to infer its functioning and extract their secret by inspecting the supply current (43). Similarly, power analysis attacks, are one of the most successful ones according to "*Power analysis attack: A vulnerability to smart card security*" (44). This attack focuses on the analysis of the power traces of the system to understand the cryptographic operations behind the hood. According to the paper, these attacks have been proved successfully against AES, DES, RSA, and ECC cryptographic algorithms used in smartcard applications.

Another interesting threat the authors mention is rogue terminals. In this type of attack, users interact with a seemly official terminal that might charge more without the user knowing. The best countermeasure is to apply the right controls to ensure that communication is only allowed between authenticated entities, which can be done through cryptographic operations and secret keys.

The paper "*User Privacy in Transport Systems Based on RFID E-Tickets*" (45) expands on the potential attacks on ticketing systems. These are impersonation, tracing, and DDoS. Impersonation attacks involve attempting to access the system by unauthorized individuals through obtaining or simulating a valid ticket/token. These attacks involve man-in-the-middle or replay attacks.

Man-in-the-middle attacks occur when a malicious actor eavesdrops on communication between two parties, which in our case is the user and the server. If the connection is not properly secure, the attacker might access the unencrypted data, thus viewing confidential data or Personally Identifiable Information (PII). Not only that, but the attacker could also intercept the traffic flow and modify it on the fly.

Tracing affects the privacy of users in the way that companies attempt to identify patterns to improve their services. These data analyses can identify users as their cards are often linked to a special UID or token. Transport authorities can then link a token to a user and understand their behaviour and movement patterns. This translates to a loss of the user's privacy. However, this not only affects transport authorities but also if the token were to land in the wrong hands, it could then be used to trace passengers by malicious entities.

Distributed Denial of Service (DDoS) is a form of attack where multiple devices coordinatively interact with a system to saturate its services and computing power to make it unavailable to legitimate users. In our context, that means threat actors exploiting weaknesses in protocols so that valid tickets are no longer accepted or the system becomes unavailable.

Another kind of attack is considered in the paper "*Lightweight cipher algorithms for smart card security: a survey and open challenges*" (46) is an insider attack. This attack originates from authorized users within the system that have easier access than external parties. These users already have access to the system and, if the proper controls are not implemented, they might have more privileges and access than required and could end up accessing PII data or extracting secrets from the smartcard or ticketing scheme, intentionally or not.

To protect against these types of threats and vulnerabilities, cryptographic algorithms are applied to the information stored on smartcards. Even though some of the literature reviewed and presented in the paper "*Lightweight cipher algorithms for smart cards security: a survey and open challenges*" make use of a PIN or OTP through SMS for authentication, this implementation is not suitable for public transportation as it needs fast interaction and processing to access the transportation network. The use of PIN would generate a queue for each user to enter their smartcard and associated PIN.

In the paper "*Cryptographic algorithm optimization*" (47) the authors designed an implementation of Hummingbird cipher for smartcards. This is an ultra-lightweight cipher that is a hybrid between block and stream ciphers. The authors identified an optimization of the implementation from the power and area perspective in that the asynchronous mode of the algorithm is better for smartcards by using 4 substitution boxes instead of 1, therefore consuming less power and processing time.

In the paper "*Comparing and implementation of public key cryptography algorithms on smart card*" (48) the authors compared the application of ECC and RSA for data encryption on smartcards. They concluded that ECC is better suited due to using a small number of keys than RSA and using fewer hardware resources and bandwidth.

User privacy

Concerning privacy concerns, most ticketing systems issue passes that contain a unique ID number that can be linked to the pass's owner. To offer seasonal tickets, it is common to have users register within an application to be issued a card that contains PII information such as Name, Surname, and a picture. This information is not only stored on the microchip of the card but it is also printed on the card itself, either on the front or the back of it. It is obvious that this information is accessible by anyone that has a visual of the card, but, on the technology side, the information contained in the microchip is only accessible by the ticketing system (or issuer transport authority or operator)

The paper "*Privacy-preserving Public Transport Ticketing System*" (49) mentions how digital travelling passes are often linked to a unique ID that represents the identity of their owners. This is especially true for those personal transport cards that require registration with personal data. However, for passengers that are privacy-aware, anonymous transport cards could be used. Even though the identity is not given in these

types of cards, powerful data mining techniques could be used to determine who the owner is.

For this privacy scheme, the authors propose the use of Zero-knowledge proofs so that one party can convince the other party they know a certain value or secret without revealing it. This, for instance, would allow passengers to prove certain attributes such as birthday, older than 18, etc. without disclosing those details to the transport authority.

The authors present a smartphone application that allows users to buy single tickets and seasonal passes upon registration with the transport authority but without revealing details to them. Firstly, users must interact with the ticketing application to obtain an anonymous credential.

The application interacts with the ticketing systems. Upon entering a transport service, the application contacts the transport authority to request a ticket by proving the passengers had purchased a ticket or pass and it is still valid. This ticket is then validated at the machine on the bus or train.

In the paper *"Privacy-preserving billing for e-ticketing systems in public transportation*" (50) the authors demonstrate an attack to retrieve passengers' details from the smartcard EZ-Link used in Singapore. This is caused by the travel records being sent in the clear between the NFC reader and a PC, and between the PC and EZ-Link servers. The authors propose a practical attack where an NFC reader is hidden and then comes into contact with an EZ-Link card. This reader must be connected to the internet to then retrieve the passengers' most recent travel history. The authors also claim that the EZ-Link reader does not perform any cryptographic operation as it simply acts as a relay between the smartcard and the PC.

Mobile payments

Mobile payments have taken the world by storm by enabling users to use their smartphones to pay at merchants, supermarkets, transport services, and essentially, anywhere that accepts bank card payments. In the context of public transportations, passengers can now access buses, trams, trains, and metro by simply tapping their devices.

There are several ways in which users can access public transportation systems and these come down to the implementation of the ticketing system. These alternatives are visual inspection, QR code, and NFC.

In the first one, users are given a digital or physical ticket upon paying for a transport service online or physically on trains or buses stations. Upon accessing the transport mean, the digital ticket is visually inspected by a member of the staff to grant access. In the second one, passengers are given a digital ticket with a QR code after booking a trip, these QR codes are then scanned at either a turnstile or a QR scanner placed in the transport mean. Finally, NFC allows users to access transport services by simply tapping their devices on a compatible NFC terminal. Depending on the transport

authority, the terminal can be interacting with an emulated bank card or with a transport card through HCE.

It's evident that the first mode introduces a privacy concern as for a staff member to visually inspect the card or ticket, it must have the owner's details written on it. In the event of theft or loss, unauthorized parties could then view the cardholder's name, surname, and passport photograph. Another visual inspection could be performed should the ticket be stored on a mobile phone; the inspector would need to verify its validity. Some transport authorities do not trust screenshots due to counterfeit images and only trust tickets shown through an application developed by them like in Greatest Western Railway or First Bus services in the UK (51). These often include an animation to show the app is running in real-time. This visual inspection could be subject to a replay attack where an unauthorized party record the legitimate screen and then replay it to the inspector. Threat actors could develop similar apps that mimic the feeling of the trusted one, therefore, it might be difficult for staff members to distinguish the real from the fake one.

There is also another risk of using smartphone apps which are trojan horses or non-official but seemly official apps. Users' PII and payment information could be leaked should they inadvertently give their credentials to threat actors as discovered by Symantec researchers when the Uber app on Android was targeted. (52)

QR code also has its security concerns as outlined in the paper "*QR Code Security*" (53). Attacks involving QR codes can be placing a malicious QR code on top of a legitimate one mimicking its surrounding appearance. Another one involves buffer overflows and underflows by modifying bits that indicate the character count. Buffer overflows attempt to overwrite data to adjacent memory locations by exceeding the storage capacity of the memory buffer. On the other hand, underflows might provoke undesired side effects as the data is fed at a lower data speed than is being read from the memory.

Additionally, automatic system scanning QR codes could be vulnerable to SQL injections and command injections. If, for instance, an automatic scanning software scans QR codes that embed malicious information such as an appended SQL query, could inject into the back-end database with serious consequences, from denial of services to data leaking and full database compromise. Command injection behaves similarly so that operative systems run an unauthorized command that can download malware, open ports, enable reverse shell etc (53).

QR codes could be used to embed malicious URLs that upon scanning them take users to dangerous sites that automatically download malware in the background. This malware can take many forms and perform dangerous actions such as opening backdoors, stealing information, taking over accounts, etc. QR codes can also be the subject of phishing where threat actors create a website and/or emails that mimic the official ones but embed malicious QR codes (54).

Mobile payment through NFC presents its own set of security issues. For instance, in the paper "*Practical EMV Relay Protection*" (55) a vulnerability was discovered in iPhones using Apple pay and VISA bank cards whereby payment authorization and contactless limit could be bypassed through an active Man-in-the-middle and relay attack. For this attack to work, the iPhone would need to be set to Express Transit/travel feature, this feature enables Apple Pay users to pay transport fares without unlocking their devices for usability purposes.

Chapter 4: Standards & Technology

In this chapter, we explore the different standards, formats, and schemes that were defined to regulate the communication between the smartcards and the reader in public transportation services.

Even though most fare collection systems or simply ticketing systems implemented are proprietary (MIFARE, Sony's FeliCA) there also exist public schemes such as ITSO Specification, Calypso, and CiPurse that aim to address the interoperability of transit tickets across operators.

4.1) ISO Standard

Contactless smartcard communications are ruled by the ISO/IEC 14443 standard which defines two types of contactless cards, A and B. The main difference lies in the modulation, protocol initialization procedures, and codification schemes. Type A card uses 100% ASK modulation for the transfer of data between the reader and the card. Type B card however uses 10% ASK modulation for the same procedure.

The standard is developed by the International Organization for Standardization (ISO) and describes how contactless smartcards and terminals should operate to maintain compatibility. The standard is divided into four main sections:

- Part I: Physical Characteristics
- Part II: Radio Frequency power and signal interface
- Part III: Initialization and anti-collision
- Part IV: Transmission protocol

Part I defines the physical characteristics of smartcards. For instance, in terms of dimension, smartcards shall conform to the requirement for ID-1 cards defined in ISO/IEC 7810, which in turn, is 85,6 x 54 mm. (56) (57) The standard also defines the radio frequency used as both card types operate ad 13.56MHz frequency and support communication range up to 10 cm.

4.2) Private Technology Schemes

4.2.1) MIFARE

MIFARE is a proprietary technology owned by NXP Semiconductors, a company that used to be part of Philips Electronics. Overall, their smartcards are based on ISO/IEC 14443 Type A standard, thus operating at 13.56 MHz frequency.

In terms of security, these cards support DES, 3DES, and AES encryption algorithms depending on the MIFARE family. There are four families of MIFARE contactless cards.

MIFARE Classic

MIFARE Classic is a contactless smartcard launched in 1994 operating at 13.56 MHz frequency and ISO 14443 A compliant. Concerning memory, there were two options available 1K, and 4K EEPROM.

The card used a proprietary encryption algorithm and authentication protocol created by NXP called Crypto1 (58). This algorithm provides confidentiality and mutual authentication.

As with any proprietary item, the design details of Crypto1 are kept secret. However, it is known through technical specs that Crypto1 is a stream cipher using a 48-bit secret key.

In 2008, Dutch researchers discovered the possibility to retrieve secrets from the card, thus being able to effectively manipulate the content of it or even clone it (59) (60). To counter this finding, in 2011 NXP released a hardened version of the classic card called MIFARE Classic EV1. Nevertheless, its security was broken again in 2015.

In the paper "*Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards*" (61) they present a novel card-only attack that exploits the cryptographic weaknesses of Crypto1 cipher through the weak random number generator to retrieve the secret key in approximately 5 minutes.

MIFARE Plus

In 2008, MIFARE Plus was announced as a replacement for the MIFARE Classic cards. The main benefits of this upgrade were the use of AES cipher for authentication and encryption with 128-bit keys, EAL 4+ certification, and support ISO/IEC 14443-3A for anti-collision mechanism.

MIFARE Plus supports four different security levels, from least to most: SL0, SL1, SL2, and SL3. The first one is the out-of-the-box one where the card does not have any security configuration. SL1 emulates a MIFARE Classic card for compatibility purposes and as such, uses the broken Crypto-1 cipher.

Similarly, SL2 still uses the Crypto-1 cipher with the difference that the keys are generated by AES in the mutual authentication. Finally, SL3 is the most secure one as it does not use Crypto-1 at all, only AES (62).

MIFARE Ultralight

The MIFARE Ultralight family didn't include cryptographic protection at first. Later on, NXP released a new version called MIFARE Ultralight EV1 with enhanced security features. However, it wasn't until the arrival of MIFARE Ultralight C, a cheaper option, that a standard cipher was included. In this case, it was 3DES for chip authentication and data access. Additionally, a fourth family member called MIFARE Ultralight AES was developed to protect data based on AES with 128-bit key length and EAL 3+ certification (63).

The key tech specs of this family are:

- Fully ISO/IEC 14443 A 1-3 and NFC forum tag type 2 compliant
- Operating distance up to 10 cm, 13.56 MHz operating frequency
- Data transfer of 106 Kbit/s
- True anti-collision
- Field programmable 'Read only' locking function per page
- Up to 100.000 single write operations
- MIFARE SAM AV2 based security methods supported
- Data integrity of 16-bit CRC, parity, bit coding
- 7-byte UID – unique identifier (cascade level 2 according to ISO/IEC 14443-3)

Regarding its application, according to MIFARE this type of card is more suitable for event ticketings such as sports games, museums, loyalty schemes and limited use tickets in mass transportation that is, single or multiple trips, tourist passes but not seasonal ones.

As an example of the implementation of this type of card, the metro of the city of Malaga, Spain, uses a MIFARE Ultralight EV1 card whose appearance is depicted in Figure 11. It is a paper ticket which can be bent.

Figure 11. Malaga metro's paper ticket (64)

Upon holding the ticket against a strong light, we can see the RIFD antenna as depicted in Figure 12.

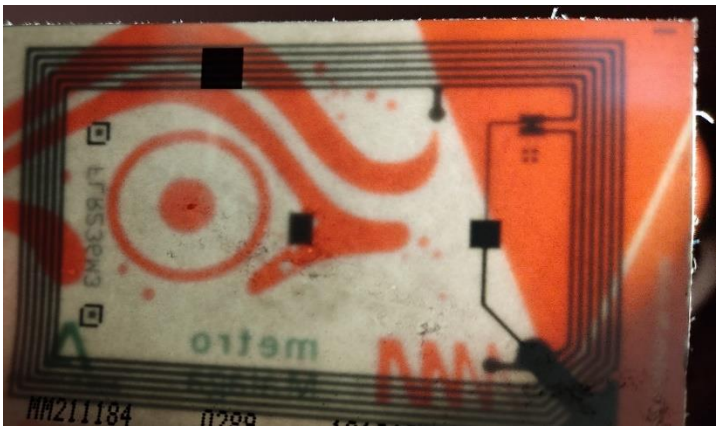


Figure 12. Malaga's metro card RFID antenna

This card was scanned using an app called NFC TagInfo by NXP Semiconductors v.2.0.7 running on an iPhone SE with iOS 14.6 to simulate what information could be read should someone find a random card on the street. Figure 13 displays the information the app can detect from the card. As can be seen, the app successfully detects the card as MIFARE technology, particularly Ultralight EV1 family. The card counts with a memory of 128 Bytes and supports ISO14443-3. Other than that, no further information was obtained through the app.

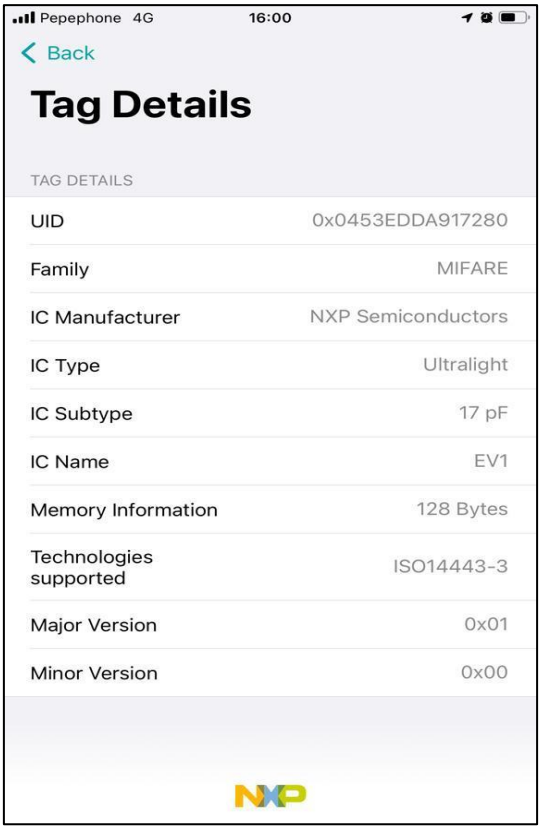


Figure 13. Malaga's card info detected by NXP TagInfo app

MIFARE DESFire

MIFARE DESFire family was released in 2002 with more security features than its predecessor, the classic family. In its initial version, DESFire card supported DES and 3DES ciphers.

This card was designed for multi-application smartcard solutions in access, loyalty program, payments, as well as advanced transport schemes. It offers quick and highly secure data transmissions.

In 2010 & 2011, however, German researchers broke the security of the original MIFARE device through a side-channel attack that could be used to clone and manipulate these cards. (65) (66). After this, the original DESFire card was superseded by MIFARE DESFire EV1.

4.2.2) FeliCa

FeliCa is a proprietary smartcard scheme created by Sony in Japan. The technology is primarily used in the public transportation services of Japan, Hong Kong, and Singapore. FeliCa is the standard smart ticketing system in Japan.

Like other formats, FeliCa smartcard does not count with a battery, so it is externally powered to operate. It uses a special FeliCa card reader that powers the card when it is in range until the transaction is complete. The technology can process transactions as fast as 0.1 seconds using Manchester coding at a transfer rate of 212 kbits/s and operating at the frequency of 13.56 MHz (67).

Concerning security specifications, initial versions of the FeliCa smartcard were certified by ISO/IEC 15408 EAL4. The cryptography algorithms used in this version were DES and 3DES. (68). Next-generation of FeliCa smartcards from 2012 onwards has achieved EAL6+ certification of Common Criteria (ISO/IEC 15408) that measures IT security. This new generation includes AES in addition to the existing DES encryption algorithms.

The encryption key is dynamically generated each time the mutual authentication process is performed, hence, reducing fraud. FeliCa's communication system is compliant with ISO/IEC 18092 standard, which defines NFC. In terms of wireless communication protocol, Felica conforms to ISO/IEC 14443 (67).

4.3) Ticketing public Standards

4.3.1) ITSO Limited

ITSO Ltd is a non-profit organization in the UK whose goal is to make access to transit services as easy and seamless as possible via smart technology throughout the UK. To achieve this, it released the ITSO Specification which became the national standard to regulate the interoperability of tickets across public transport operators in Great Britain (69).

The main idea is that public transport operators' systems can talk to each other so that passengers can use a single ticket regardless of the operator that issued it or is providing the actual service. ITSO also operates a testing and certification service to guarantee that the smart ticketing equipment is ITSO compliant.

All ITSO compliant system relays on ITSO Secure Application Modules (ISAM). These are programmable chips used in every POST (Point of Service Terminal) and Host Operator Processing System (HOPS/back office).

The ITSO environment includes the following elements:

- Smartcard or smart device
- POST (ticket machines or barriers)
- HOPS (back-office processing system)

ITSO operates the ITSO Security Management Service (ISMS). This system provides key management facilities in a secure datacenter, manages lifecycle cryptographic keys, ensures the ISAMs are configured securely with these keys as well as manages the lifecycle of ISAM. In this way, ITSO assures the integrity of the member public transport operators' systems.

To communicate with the ISMS, each user is required to have an Asset Management Service (AMS) function within a HOPS. All ticketing machines, automated barriers, and HOPS under ITSO scheme contain an ISAM that securely stores the cryptographic key.

4.3.2) Calypso Networks Association

Calypso is an open global security standard for fare collection systems suited for mass transportation systems which aims to cover modern mobility needs in smart cities. The idea behind the standard was born back in 1990 by a group of transport operators such as Innovatron, RATP, and SNCF which shared the common goal of creating a non-proprietary standard for a secure, flexible, and fast mass transit ticketing system. (70)

The standard operates through contactless smartcards or contactless compatible devices and has been successfully implemented in 25 countries including Portugal, Italy, France, Mexico, Belgium, Morocco, and Israel.

The Calypso smartcard proposed in the specification is designed for either payment or access to services including public transport. The card itself is compliant with ISO 14443 for contactless communication, ISO 7816-3 if embedded in a smartcard format, and ISO 7816-4 for commands and file types. As it complies with ISO 14443, the communication takes place at 13.56 MHz frequency.

The specification defines a secure contactless system composed of a central system, which tracks transactions, a reloading system that allows to top up cards and adds tickets to them, a validator system that grants access to transport services, and

optional devices for controlling purposes such as an inspector checking a passenger has a valid ticket. (70)

Concerning security, the standard defines the technical specification for secure and fast contactless communication between a contactless device and a terminal. Essentially, the security of the system is provided through cryptographic algorithms with secret keys stored in both the cards themselves and in Secure Application Modules (SAM). The secret keys are embedded in the smartcard at manufacturing time, as well as the application data. (70)

The SAM is presented as a smartcard of the size of a regular mini-SIM card that is permanently stored in the terminals that interact with the passengers' smartcards. In terms of the cryptographic algorithms, the specification defines the use of the following ones:

- AES with 128-bit key
- DESX with 120-bit key
- 3DES with 112-bit key

It is worth noting that DESX is used to prevent brute force attacks on DES cipher by increasing the key size by 8 bytes. These algorithms are used to prevent card cloning and unauthorized top-ups.

The specification defines three different secret keys: the issuer key, the load key, and the debit key. The first one is used to modify the data of an application at a global level, the second one is often used as a reloading key, and the last one serves as a validation to verify the value of the card. All these three keys are 16 bytes and are used by the ciphers mentioned above.

These secret keys are stored in both the card themselves and a Secure Application Module (SAM) located in the terminals. These keys allow to authenticate the card and modify the data in them. To interact with a card, each terminal must be equipped with a SAM. However, it must also implement some controls to limit the actions terminals can take on the cards. For enhanced security, the keys stored in the card are diversified from a master key, which translates to each card having different key values.

The specification defines a mechanism called secure Session to prove the card is genuine, and to ensure the integrity of the data written to it. This session is established between the card and the terminal with a specific command called "*Open Session*" and it is closed by the command "*Closed Session*". This session allows the terminal to read from and write to the card. Upon session closure, the data is signed by both the card itself and the SAM in the terminal, thus proving the authenticity of both the card and the terminal, as well as the transaction (70).

Concerning integrity, the Calypso smartcard protects the integrity of the transactions to prevent corrupt data. For instance, in the event of power loss such as removing the card from the terminal before the transaction is complete, an auto-

recovery mechanism is used to roll back to the card's previous state. If the card is not able to fully validate the transaction, the changes are discarded.

4.2.3) CiPurse

CiPurse is an open security standard for public transport fare collection systems using smartcard technology. This standard was first developed by the OSPT Alliance in 2010 and has evolved ever since. The main idea behind it is to have standardized fare collection systems that ensure interoperability concerning fare payment and public transport access. It promotes vendor neutrality and interoperability across vendor systems.

The standard is built on industry standards such as AES-128, ISO/IEC 14443, and ISO/IEC 7816-4. It supports payment media such as contactless cards, wearables, and mobile payments, whether using a Secure Element or HCE (71).

Below are the components of this standard:

- **Core Specifications**
  Standardized the interfaces, crypto functions, and operations of each profile to guarantee interoperability and security

- **Profiles**
  Specifies the level of complexity and functionality of a CiPurse solution.

- **Terminal Specifications**
  Defines the CiPurse SAM, SAM use cases, and a guide to key management.

- **Mobile Specifications**
  Details about how to support CiPurse in a mobile environment.

- **Java Card RTE Specifications**
  Details about the Java Card Server Crypto API for both terminals and readers.

4.2.4) CEPAS

CEPAS or Specification for Contactless e-Purse Application SS 518:2006 is a Singaporean standard for electronic money stored in a smartcard. The standard defines the main commands used to interact with e-purse applications, which are "*debit*" and "*credit*". The former is used to decrease the value of the card whereas the latter is to increase it. In addition to them, there is another command called "*Read purse*" used to retrieve information from the card.

CEPAS closely follows international standards ISO/IEC 9797-1 and ISO/IEC 7816-4. CEPAS also includes an integrity protection mechanism to ensure that

modifications to the card are either completed or discarded, thus data corruption or inconsistent states do not occur. In terms of security, CEPAS proposes the use of 3DES.

Chapter 5: Real-World Integrations Review

This section aims to briefly review some of the multimodal transportation systems implemented in cities around the world. Table 3 below summarises the key details of each system reviewed.

Table 3. Multimodal Transportation systems used around the world

Name	Uses	Since	City	Country	Technology
Octopus System	MTR Buses MTR Light Rail Ferries Taxis Tram Trains Shops	1997	Hong Kong	Hong Kong	FeliCA
Oyster	London Underground London buses TfL Rail Trams Ferries National Rail Services	2003	London	UK	MiFARE
Navigo	Metro Train Bus	2001	Paris	France	Calypso
Suica	Train Bus Tramway Vending machines Shops	2001	Tokyo	Japan	FeliCA
MetroCard & OMNY	Buses Lightrail Subway	1993 & 2019	New York	USA	Magnetic Stripe & MiFARE
Opal	Bus Train	2012	Sydney	Australia	MiFARE
EZ-Link	Mass Rapid Transit Bus Light Rail Transit Parking facilities Vending machines	2002	Singapore	Singapore	FeliCA & CEPAS

5.1) Octopus System (Hong Kong)

Hong Kong was one of the first cities to implement the use of contactless smartcards in their mass transportation system. The system and card are both called Octopus and it has been used since 1st September 1997.

In 1994, ERG Group (today Vix Technology) was selected to design and lead the development of the Octopus system as well as for building and installing its components. The business-as-usual (BAU) operations and maintenance were performed by Octopus Cards Limited.

At first, Octopus cards were used to pay transportation fares granting access to MTR Buses, MTR Light Rail, ferries, taxis, trams, and trains. Since its adoption, the Octopus card has evolved to include payments in supermarkets, convenience stores, fast-food restaurants, petrol stations, vending machines, parking meters, and many more (72).

There are two main types of cards available in the Octopus Systems: on-loan cards and personalized cards. On-load cards are primarily used for fare payment in the public transport system, and they are completely anonymous. No information such as bank details or personal data is stored in the card and no ID is necessary to purchase them. On the other hand, personalized cards are indeed tailored to the individual and as such, are available upon registration.

Figure 14 below shows the appearance of a regular Octopus card for Adults issued from 2017 onwards. The card depicted is of the type “on-loan”. As can be seen, no personal details are printed on the card.

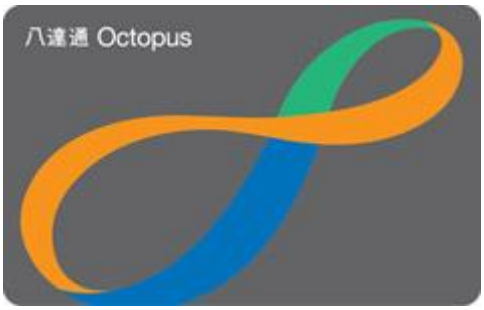


Figure 14. Standard Octopus Card for Adults since 2017. (73)

5.1.1) Technology

Regarding its technology, Octopus cards were developed by Sony and use their 13.56 MHz FeliCa RFID Integrated Circuit (IC) chip. This chip permits communications between the card and the payment processor using a reader/writer device. This device has an antenna and a processing board so that physical contact between cards and the reader is not necessary, users only need to place the card near the device. The reader ranges go between 30 mm and 100 mm depending on the model used.

Reader devices do not have real-time round-trip comms with the central Octopus computer, instead, the system uses a Store and Forward method whereby the data is stored within an intermediate station and later transmitted to the central Octopus computer for settlement (72).

5.1.2) Security

Concerning its security, the Octopus System uses a modified version of the three-way handshake mutual authentication protocol defined in ISO 9798 for communications between the card reader and Octopus cards (74). In this way, both parties can check the other's identity.

As mentioned before, the communication does not require physical contact and as such, the communication is airborne. This path between the reader/writer device and the Octopus card is also protected using a pair of transactions key and ID whose generating occurs randomly at the beginning of every communication session (74).

To achieve confidentiality of the Octopus System, 3DES is used during the mutual authentication process. The communication channel is only established when the card and reader have authenticated each other based on a shared secret access key. The security of the system could be in danger should this secret key be compromised.

5.1.3) Smartphone App

Octopus Cards Limited developed an official smartphone app for the transport system called Octopus App. It is available for Android and iPhone devices, and it allows users to manage both Octopus cards and Octopus Wallet. Users can top up their cards with money in the Octopus Wallet or directly from their bank accounts.

On 14th December 2017, the cardless Smart Octopus was implemented to allow mobile payments through the Samsung Pay platform. This payment method uses NFC and MST technology so that users can simply tap their Samsung devices on the Octopus reader. Similarly, Huawei users can leverage Huawei Pay to seamlessly access the transport system or pay in shops.

In addition to Samsung Pay, Apple Pay was implemented on 2nd June 2020 for compatible Apple devices. As Octopus System uses Sony's FeliCa technology, only iPhone 8 and upwards and Apple Watch 3 and upward are supported.

5.2) Oyster System (London, United Kingdom)

In London, the implementation of the Oyster ticketing systems allows passengers to seamlessly access the different public transportation means the city has available. With an Oyster card, users can access the London Underground, London buses, TfL Rail, Trams, ferries, and National Rail Services.

The main component of the Oyster system is the Oyster card. This is a contactless smartcard that acts as a wallet that users can top up to travel around the Greater area of London (75). It was first introduced in June 2003.

Figure 15. London Oyster Card (76)

As part of the Future Ticketing Program in London, Oyster payment has been supplemented with contactless bank cards, mobile devices and smartwatches using Apple Pay, Google Pay, or Samsung Pay. Users can leverage NFC technology to seamlessly access the Transport for London (TfL) services through their Android, Apple, or Samsung devices.

In July 2015, Apple Pay was introduced in the TfL network as the first mobile ticketing option for compatible iOS devices. It worked similarly to regular Oyster cards in which users only needed to hold their iOS device near the Oyster reader. (77)

The second mobile payment option was introduced in May 2016 with the integration of Google Pay. Android users with compatible devices could now access TfL services by tapping the top half part of their smartphones on the Oyster card reader (78).

On 16th May 2017, TfL announced the integration of Samsung Pay as a mobile ticketing option to access London's transport network. Samsung worked closely with TfL to allow Samsung Pay users to designate a specific bank card as a transport card to use whilst travelling on TfL network (79).

5.2.1) Technology

The blue Oyster card counts with RFID technology under the hood. Its proximity range is about 80 mm, and the RFID system is compatible with ISO/IEC 14443 types A and B. Oyster cards issued before February 2010 had a MIFARE Classic 1k chip, which was discontinued due to weakness whereby cards could be cloned or even the amount held in the card could be modified (80)

MIFARE Classic chip was replaced by the more secure MIFARE DESFire EV1 chips. These new chips had more computing power as well as more sophisticated security features.

5.2.2) Smartphone App

In 2017, TfL made the Oyster card app available to customers using Android or iOS devices free of charge. This app allowed passengers to check their journey history, top up their cards, and buy seasonal tickets.

5.3) Suica Card (Japan)

There exists ten major transport operators covering different Japanese regions that issue independent contactless smartcards. In 2010, they decided to establish an IC Card Inter-Operator Centre to achieve interoperability so that users could travel around Japan with any of the contactless smartcards regardless of whom issued them.

JR East launched the contactless smartcard Suica in November 2001. It works like a prepaid e-money card that acts as a digital purse. Users top up its value and then a fare is automatically deducted when tapped on a terminal. Suica not only allows users to access transport services but also to purchase items from vending machines, station kiosks, and convenience stores.

The overall appearance of a Suica card is depicted in Figure 16 below.

Figure 16. Suica card (81)

There are two versions of the Suica card that can be obtained through ticket machines but the main difference depends on the information provided to get them. The general version does not require any user information, it is completely anonymous. The personalized version however is only available prior registration. Users that aim to acquire it need to provide personal information such as name, surname, gender, telephone number and date of birth. Once printed, the personalized card includes the cardholder's name and surname on the front.

The technology behind the Suica card is Sony's FeliCa which as we have seen is a proprietary smartcard scheme and the defacto technology for smart ticketing systems in Japan. Sony's website mentions FeliCA cards use AES and DES but does not include further details about them, such as key length. This technology however has achieved an Evaluation Assurance Level (EAL) of 6. EAL evaluates the security of IT systems and assigns a numerical value between 1 and 7, the higher the better as it shows the system's principal security components have been reliably implemented.

5.3.1) Smartphone App

There exist a digital alternative to the physical Suica in the form of a smartphone app. Users can generate a brand new digital Suica card or import its physical one. This

app is called Mobile Suica and it is available for both iOS and Android. The English version is called SuicaEng and it is very limited compared to its Japanese counterpart.

Alternatively, the Suica card is compatible with Google Pay and Apple Pay. For Android users, this system is only available for users living in Japan and requires Osaifu-Kentai eligible phones to import the Suica card.

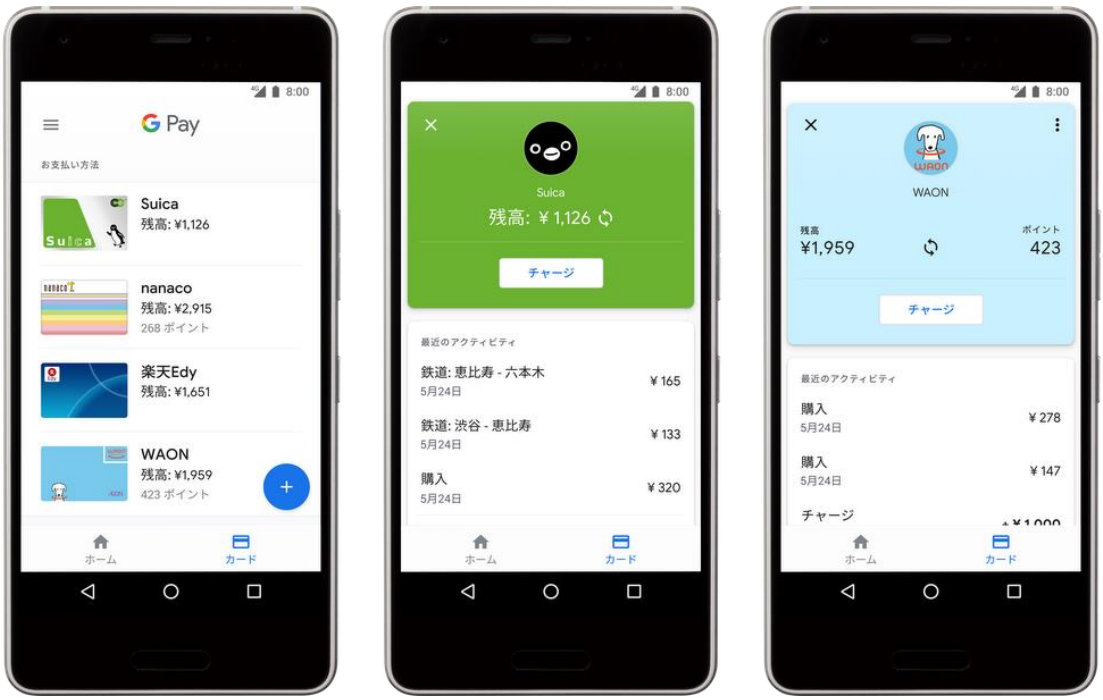


Figure 17. Suica Card in Google Pay (82)

Apple Pay users do not have the limitation of having to live in Japan when using an iPhone 8 or later, whereas iPhone7 users must have purchased their devices in Japan. Then, users only need to add their Suica card to their Wallet App on Express Mode. This mode allows the use of the Suica card without unlocking or waking the device.

5.4) EZ-Link (Singapore)

EZ-link card is a contactless smartcard introduced by the Land Transport Authority in Singapore in April 2002 for public transit use on buses, MRT, and LRT. Its acceptance grew in popularity, and it is nowadays accepted in both public transit and private transport providers such as buses, taxis, metro, and cruises.

Figure 18 EZ-Link contactless card for adults (83)

5.4.1) Technology

When it was first launched, the EZ-Link card made use of Sony's NFC FeliCA technology. However, in 2009, the Land Transit Authority decided to move toward its technology standard called CEPAS (Contactless e-Purse Application Specification).

CEPAS is a Singaporean specification developed by the Infocomm Development Authority of Singapore (IDA) to have a single card for use all around Singapore for micro-payments (transport, taxi, retail, etc.). This standard focuses on the interoperability of card payment schemes from different companies and system operators (84). This technology expanded the card use to car parks, taxis, supermarkets, convenience stores, etc.

Additionally, it is possible to pay transit fees by simply using your phone's NFC functionalities. However, it is not as easy as it seems at first it is needed to buy a SIM card from a Singaporean service provider called EZ Link NFC Sim that acts as a purse.

In addition to the cards, EZ-Link has developed a series of collectable charms and wearables with contactless technology with the same functionalities as a regular EZ-Link card. Some examples of these charms are included below:

Figure 19. Harry Potter EZ-Link Charm (85)

Figure 20. Captain America EZ-Link Charm (85)

5.4.2) Smartphone app

It has an app called “EZ-Link” that allows users to top up their cards through NFC as well as access to their EZ Wallet. This wallet was launched in March 2020 and allows users to pay through a generated QR code on the app.

Users top up the wallet with a regular bank card and then scan the QR code at a retail shop and enter a payment amount. The payment is authorized by entering a 6-digit Pin or using the fingerprint scanner on the phone (86). The app is available through main app stores such as App Store, Google Play, and Huawei’s AppGallery.

5.5) Navigo Card (Paris, France)

The Navigo card (formerly Navigo pass) was introduced by the Île-de-France Mobilités (IDFM) transportation authority in October 2001 to cover transport in the City of Paris and the Île-de-France region. Its main component is a contactless smartcard-based on the Calypso standard leveraging NFC technology.

Figure 21. Navigo Card (87)

Additionally, in 2018 the transport authority added a mobile phone app called Vianavigo for users to manage their Navigo card and access transport means. The Navigo card grants holders to travel on Metro Lines, Tramlines, buses, funicular, and train lines. In addition, annual subscribers can rent a self-service bike (88). The Navigo card contains the user’s data as it is only available upon registration.

5.5.1) Technology

Calypso standard is an open standard for ticketing systems. Even though the specifics of the cryptographic algorithms are kept confidential, the following information was obtained by reading the Calypso Standard public documents. Its uses DESX, AES, and Triple-DES cryptographic algorithms.

DESX is used to fight against brute force attacks on the DES algorithm, it works by simply adding 8 bytes to the key size. Diversification is applied to increase the security of the system, that is, each card has unique keys so if a card were to be compromised, the keys of other cards remain unknown. According to the standard *"the keys of each card are computed from a master key. Generally, the card key is computed by a cryptographic operation on the application serial number, using the master key"* (89)

5.6) MetroCard & OMNY (New York City, USA)

The public transportation services in New York City are operated by the Metropolitan Transportation Authority (MTA) which provides subways, buses, and railroads services to more than 8 million New Yorkers.

Since 1993, MTA network users have used a magnetic stripe card called MetroCard to access transport services. It does not require any registration so personal data is not stored within the card. Users can buy it anonymously at MetroCard ticket machines available in most subway stations as well as selected merchants (90).

Figure 22. New York City MetroCard (91)

In 2007, a step forward occurred in the ticketing system with the adoption of contactless payments and ticketing systems. As a result, the new payment system was called OMNY (One Metro New York) that comes to replace MetroCard completely by 2023. The OMNY system is designed by the same company that developed the Oyster card, Cubic Transportation System. The actual technology used is licensed from the Oyster card system. The system will accept contactless bank card payments as well as mobile payments. Google Pay and Apple Pay are supported (92).

As with most smart card systems, privacy concerns arise regarding the lack of privacy regulations in the OMNY system. It is of concern that trip data could be accessed by the US authorities for surveillance purposes.

5.7) Opal System (Sydney, Australia)

The Opal System is the fare collection system for public transit in the state of New South Wales (NSW), mainly covering the greater Sydney area and other urban areas in NSW. It was first launched in December 2012 by the NSW's transport authority, Transport for NSW.

Opal users can seamlessly access public transit services such as NSW's metro, ferry, bus, train, and light rail services. The system was designed by Cubic Transportation Systems and the technology is based on MiFARE DESFire EV1.

Figure 23. Opal Card (93)

Contactless payments through a bank card or linked device are also accepted in Transport for NSW's network. Its usage is similar to regular Opal cards, simply place the bank card or your compatible device on top of the Opal reader to get in & off the transport. Digital wallets are also accepted so that users can simply link their bank cards to their Google Pay or Apple Pay accounts and then tap their compatible devices on the Opal reader. In 2021, Transport for NSW tested a mobile digital version of an Adult Opal card stored in the digital wallet of your phone.

An Opal card was scanned using an app called NFC TagInfo by NXP Semiconductors v.2.0.7 running on an iPhone SE with iOS v14.6 to understand what information could be extracted from the card. Figure 24 depicts the information the app can detect from the card. As can be seen, the app successfully detects the card as MIFARE technology, particularly DESFire EV1 family. The card counts with a memory of 4096 Bytes and supports ISO14443-4. Other than that, no further information was obtained.

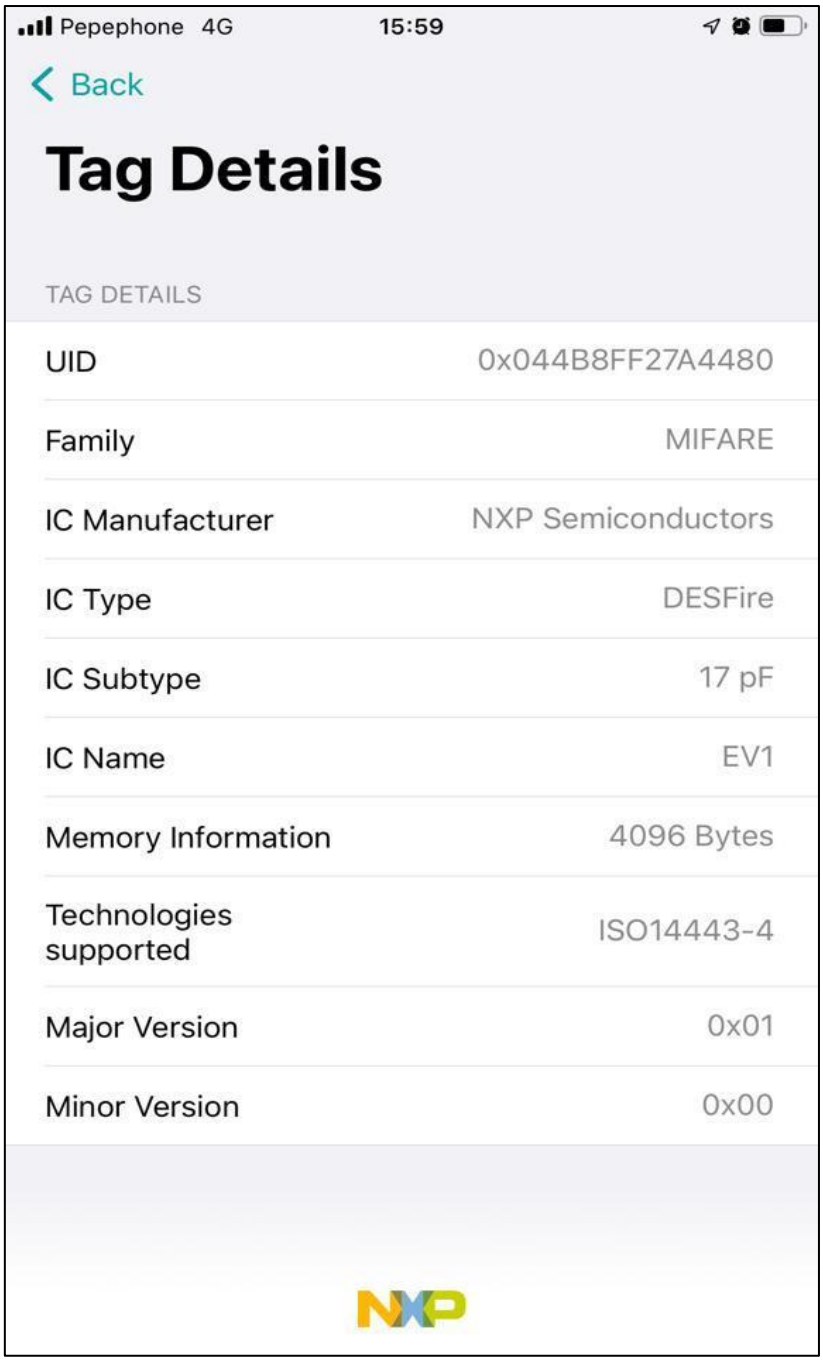


Figure 24. Opal Card's info detected by NXP TagInfo app

Chapter 6: Madrid Transport System Analysis

This section aims to provide an in-depth analysis of the technology and security of the ticketing system used in the public transportation system of the city of Madrid, Spain.

6.1) History of Madrid's Ticketing System

The beginning of public transportation services in Madrid started in 1843 with several coach services known as "omnibuses" (94) . Later in 1871, tram services pulled by mules were introduced whose fare was still paid in reales. Ten years later, pesetas started to be widely accepted as fare payment, and in exchange, a ticket was provided to the passenger as proof of payment.

With the arrival of electricity, tram services became the most important means of public transport in Madrid. During the first two decades of the twentieth century, tramways belonged to different companies so fares would depend on the conditions of the concession to each company.

In 1919, the Madrid metro opens its first line between Sol and Cuatro Caminos. Tickets are issued from the station of origin and the fare varies depending on the distance travelled. These tickets were visually inspected by a vehicle conductor and punched with a machine that validated the ticket.

Fast forward to 1970, the first automatic Metro Ticket vending machines are installed. In 1985, the Madrid Regional Transport Consortium (CRTM) is created to integrate the management of the different means of transport available in the city. That is, fare integration and considering different transport modes as part of the same network. The ticket had a magnetic strip storing the data.

In 2003 the transportation authority Regional Transport Consortium (CRTM) started a contactless card aimed to replace the traditional paper ticket. This implementation phase lasted until 2017 when the paper ticket disappeared.

In 2012, the magnetic strip tickets are replaced by a contactless smart card. In 2015, the first trials are started to test accessing CRTM's transit network through mobile phones and its NFC technology.

6.2) Smartcard Types

There exist four main contactless cards to access CRTM's transit services:

Multi-Card

It is a multi-personal reloadable card that can hold multiple tickets but seasonal ones. It is valid for 10 years after its issue date and it can be acquired in any train or metro station at one of the vending machines.

The card itself is anonymous as it does not contain any information capable of identifying the owner nor does it require prior registration with the transport authority. Figure 25 depicts the appearance of a multi-card, and as can be seen, it does not contain any cardholder information printed on it.

Figure 25. Madrid's Multi-Card (95)

Personal Card (TTP)

A personal card valid for 10 years after its issue date. It is reloadable for both personal and non-personal tickets and passes. This card can only be acquired after registration with the transit authority.

This type of card can contain multiple passes such as a defined number of tickets or a seasonal one i.e. monthly pass. As can be seen in Figure 26, this type of card contains the owner's name, surname, photograph, and also de card ID printed on the card.

Figure 26. Madrid's TTP card (95)

Children Card

The children's card is like the TTP one in terms of functionalities and details printed on the card. It can access public transport services of the Community of Madrid free of charge until the children turn 7. At this point, the card becomes invalid. Like the TTP card, children's details are printed on the card as depicted in Figure 27.

Figure 27. Madrid's Children Card (95)

Blue Card

The blue card is a special type of card similar to the regular TTP card in terms of appearance and functionalities, but it can only be used by Madrid's residents that meet certain criteria such as age or disability requirements. Figure 28 depicts the appearance of the card and like other personal cards it has the details of the owner printed on them.

Figure 28. Blue Card (95)

6.3) Access

CRTM's transit network is composed of the urban metro, bus, and suburban rail network or commuter train (Renfe Cercanias). Each of them has different fares and access methods.

Metro

Madrid's metro has an access system with barriers whereby access is granted after validating a ticket. To this effect, the turnstile has a built-in automated fare collector so that passengers can simply tap their contactless card to access the system. Each metro station has turnstiles that check the validity of the travel pass and will only open if the user has a valid ticket. In this way, human supervision is reduced.

Figure 29 depicts the turnstiles installed in Gran Via station. These count with TFT panels that informs users of the validity of the pass, as well as its expiry date or the number of remaining tickets. These systems are only implemented in a few metro stations as part of the 4.0 upgrade.

Figure 29. Metro Madrid Turnstiles (96)

The system only requires passengers to validate the ticket once, that is, at the station of origin. It is not necessary to tap the card again to exit the Metro. Normally, turnstiles would look as depicted in Figure 30. Aside from the noticeable appearance overhaul, one of the key points that set the new ones apart is the feedback provided to the user.

Old turnstiles would only inform passengers about how many tickets are left on the card but not when the seasonal ticket would expire. New ones however provide this info.

Figure 30. Madrid's metro turnstile

Bus

EMT buses accept traditional cash alongside e-payment. In contrary to the Madrid metro access to this system is without barrier. Instead, the driver makes sure that every passenger has paid by either collecting cash and providing a ticket in return or listening to the "beep" sound when a payment is validated by the contactless terminal. Like Madrid metro, EMT buses do not require passengers to tap their cards again to exit the vehicle. Figure 31 displays the payment terminal installed on EMT fleet. These terminals accept contactless payments in the form of bank card, smartphones, or TTP card.

Figure 31 EMT payment terminal (97)

Train

Renfe Cercanias' trains work in a similar way to Madrid metro with regards to having barriers for access control. Access is unsupervised as passengers must validate their ticket at a turnstile prior to accessing the system. Figure 32 depicts the turnstiles installed on Renfe' train stations

In this transport mean, passengers are required to validate their ticket twice, that is, to access and to leave the system.

Figure 32. Renfe Cercanias Turnstiles (98)

6.4) Technology

The Automatic Fare Collection system for CTRM's transit network is based on MIFARE smartcard technology. The chosen one to power the system is MIFARE DESFire EV1.

This smartcard is a passive RFID TAG, as such, it does not contain any internal power source and must be powered by a magnetic field provided by the terminal (reader). Within passive tags, there is a further distinction based on the frequency they operate: High-frequency and Low-frequency. A high-frequency card is often referred to as NFC and is the case of DESFire EV1.

MIFARE DESFire EV1 was released in 2006 and came to replace the prior MIFARE DESFire card due to a vulnerability to side-channel attacks. (99) The main difference between DESFire EV1 and the original is the inclusion of a True Random Number Generator (TRNG) and support for AES-128 encryption. Originally, the DESFire card only supported DES and 3DES. (100)

Information surrounding the MIFARE DESFire EV1 is limited due to it being proprietary. NXP Semiconductor has only released information in the form of technical

datasheets, however, the information in those documents is high-level and general, so no details of the commands used to operate the card are mentioned.

Based on the public datasheet, it was possible to retrieve the following key points:

- It has an on-chip backup management system
- Mutual three-pass authentication
- Fast data transmission of up to 848 kbit/s
- Can use 56-bit DES, 112 or 168-bit 3DES, and 128-bit AES
- Operating range: up to 10 cm
- Frequency: 13.56MHz
- Compliant with ISO/IEC 14443-4 protocol
- EAL4+ certified
- Unique 7 bytes UID for each device

The card uses an anticollision system that allows for more than one MIFARE DESFire EV1 card to be used in the nearby field simultaneously. The algorithm makes sure to select each card individually and to process the transaction successfully guaranteeing no data corruption from the interference of another MIFARE DESFIRE EV1 card nearby.

Each card counts with a unique 7-byte serial number, also known as UID located in a locked part of the memory reserved by the manufacturer. These bytes are write-protected after being implemented by the manufacturer at manufacturing time. This means the number cannot be altered later, thus ensuring the uniqueness of each card. The UID can be then used to derive diversified keys, which in turn helps to enhance the security of the card by serving as an anti-cloning mechanism.

To authenticate the transaction, mutual three-pass authentication is used between the EV1 card and PCD (Proximity Coupling Device)/terminal. Authenticating both devices in an encrypted way means they both have the same secret which confirms both entities are permitted to perform operations in each other as well as creating a session key to keep the communication path secure. This session key is generated each time a new authentication process takes place.

Security Commands

Regarding security commands, MIFARE DESFire EV1 counts with the following ones:

- **Authenticate**

- **Change KeySettings**
  Changes Master key settings on the EV1 and application level

- **Set Configuration**
  Serves to configure the card and personalize the card with a key.

- **Change Key**
  Can be used to change any key stored on the EV1 card

- **Get Key version**
  Extract the current key version of any key stored on the EV1 card

Architecture

Concerning its architecture, figure 33 depicts the overall components of the MIFARE DESFire EV1 smartcard. The architecture conforms to the diagram shown in section 2.3.1, thus having three different memories: ROM, RAM, and EEPROM, connected to the CPU. The card also counts with a co-processor for cryptographic operations and, a TRNG module as we mentioned before.

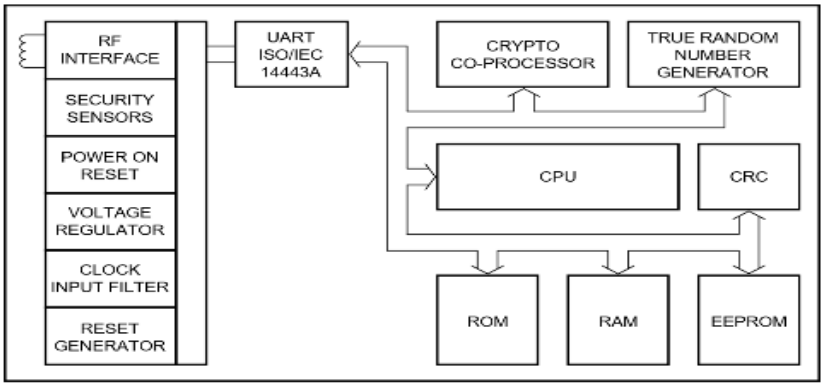


Figure 33. MIFARE DESFire EV1 Architecture

Card's shell

The card itself is made of plastic safeguarding the internal components that make it work with the overall CRTM's system. The RFID antenna alongside the chip can be spotted holding the card against a strong light as the following pictures depicts:

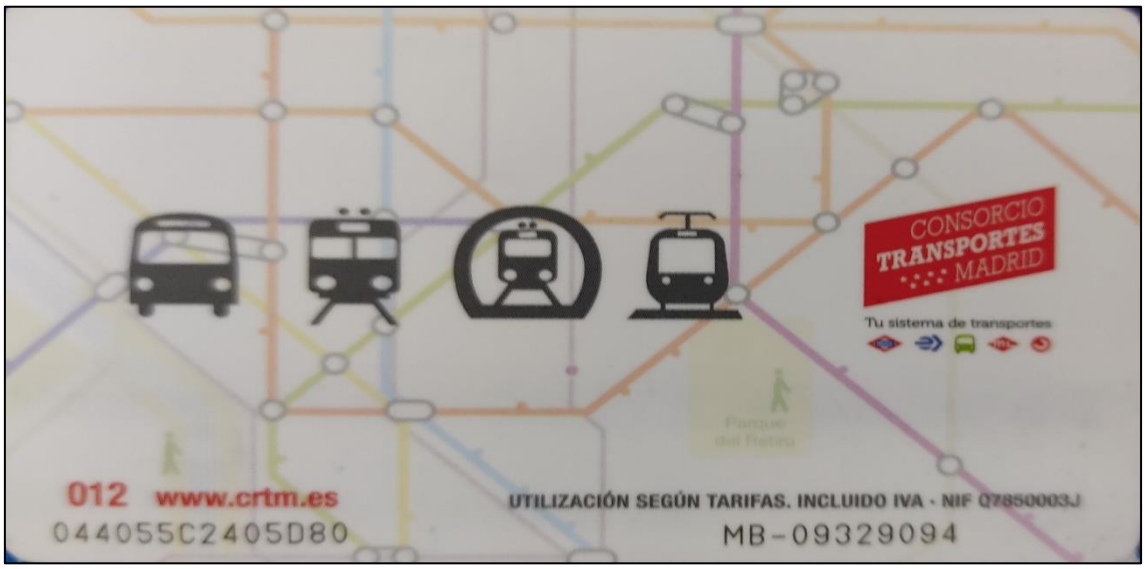


Figure 34. CRTM card's front

Figure 35. CRTM's card chip

Figure 36 CRTM's card antenna

6.5) Mobile app

In 2021, CRTM launched a mobile app called “Tarjeta Transporte” that allowed passengers to simply top up the card through their smartphone. The app is only available on Android devices and Huawei ones, but it is not compatible with iOS just yet. Through this app, users can check their number of remaining passes and tickets. It needs a data connection either Wi-Fi or comms and it needs an NFC compatible device.

Users need to register a bank card within the app to top up. First, users enter the typical bank card details such as card number, CVC code and expiration date. Then, users press pay and follow your bank instructions.

The benefit of this app is that provides information about the card itself. Otherwise, users would not be able to know whether their pass is expired or how many tickets they have left. Additionally, it adds the convenience of topping up the card anytime, anywhere, thus avoiding queues or not carrying cash.

This option however does not allow users to use their smartphone to store the seasonal pass, only to top up. Users would still need to use the card to access the services.

Figure 37. CRTM's Tarjeta Transporte app

6.6) NFC Analysis

A Multi and TTP cards were scanned using an app called NFC TagInfo by NXP Semiconductors v.2.0.7 running on an iPhone SE with iOS 14.6 to understand what information could be extracted from them. Figure 38 depicts the information the app can detect from the Multi-Card. As can be seen, the app successfully detects the card as MIFARE technology, particularly DESFire EV1 family. The card counts with a memory of 4096 Bytes and supports ISO14443-4. Other than that, no further information was obtained through the app. Similar results were obtained whilst scanning the TTP card.

Figure 38. TTP's card info detected by NXP TagInfo

6.7) Smartcard issuing

As mentioned, Madrid counts with two main types of cards, the multi-card one and the personalized one (TTP). To access greater discounts such as seasonal passes, users must have a TTP card with their details.

Multi-card can simply be obtained at one of the multiple ticketing machines located in metro and train stations, the overall appearance of these machines is depicted

in Figure 39. A passenger only needs to use the touchscreen to select the number of tickets it requires and pay the fare through either cash or contactless payment.

Figure 39. Madrid's metro ticketing machines (101)

TTP cards require users to register within CRTM's network and provide them with Personally Identifiable Information (PII). This paperwork can be done by either making an appointment at one of the CRTM's physical offices or through CRTM's website.

The online process is straightforward and requires users to navigate to https://tarjetatransportepublico.crtm.es website and fill out the form shown in figure 40 with data such as National ID number, name, surname, and birthdate. Then, the process to request a TTP card initiates and counts with four main steps as shown in figure 41:

1. Further cardholder details
2. Providing documents
3. Verifying the information entered is correct
4. Paying the fee to request the card

Figure 40. TTP request form

Figure 41. TTP request process

In the first step, aside from the data already entered, it is needed to provide a phone number, and an email address, and confirm the address the TTP card will be sent to, as depicted in Figures 42 and 43 respectively.

Figure 42. TTP request form (II)

Figure 43. TTP request form (III)

As we are providing CRTM's with sensitive information such as PII, personal documents, and processing payment through their website. The connection between users' devices and CRTM's website must be encrypted to prevent sniffing and man-in-the-middle attacks.

The typical way to provide encryption in transit for websites is to recurse to PKI infrastructure. In this way, the connection is established through a secure protocol HTTPS over port 443 thanks to an SSL/TLS certificate.

The details of the certificate used by CRTM can be easily inspected by any web browser. In our case, we used Mozilla Firefox to click on the lock button next to the URL bar to check the connection is secure, thus established via HTTPS as figure 44 shows.

Figure 44. TTP website HTTPS check

Further certificate details are depicted in figure 45. As can be seen, CRTM is using a wildcard *.crtm.es to cover all subdomains within crtm.es. The certificate is signed by the trusted authority GlobalSign. The chain can also be observed in the figure *crtm.es > GlobalSign RSA OV SSL CA 2018 > GlobalSign.

Figures 46 and 47 show other parts of the certificate not covered in figure 44. The former shows that the public key is using an RSA algorithm with a key of 2048 bits, whereas the latter shows the signature algorithm in use, SHA256 with RSA.

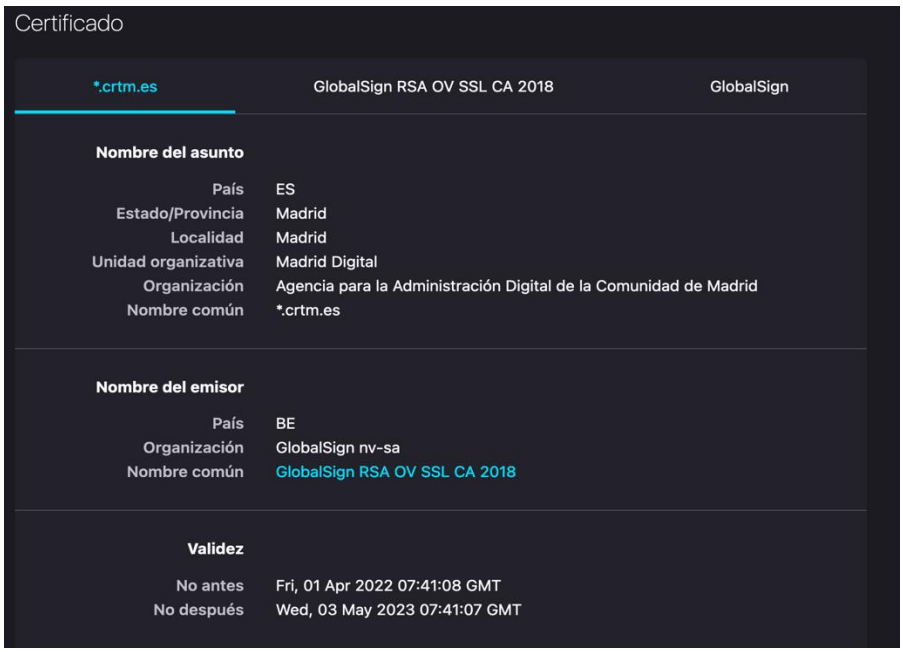


Figure 45. CRTM's SSL/TLS certificate

Figure 46. CRTM's certificate Public Key info

Figure 47. CRTM's certificate signature algorithm

A good tool to evaluate the security posture of any website is using the *SSL server test* tool provided by Qualys Lab. This is an easy-to-use and free of charge tool that checks the certificate of websites and attempts several connections to evaluate their security.

The overall result is depicted in figure 48 which shows an overall rating of B caused by TLS 1.0 and 1.1 support (no longer recommended due to weaknesses), and RC4 cipher support.

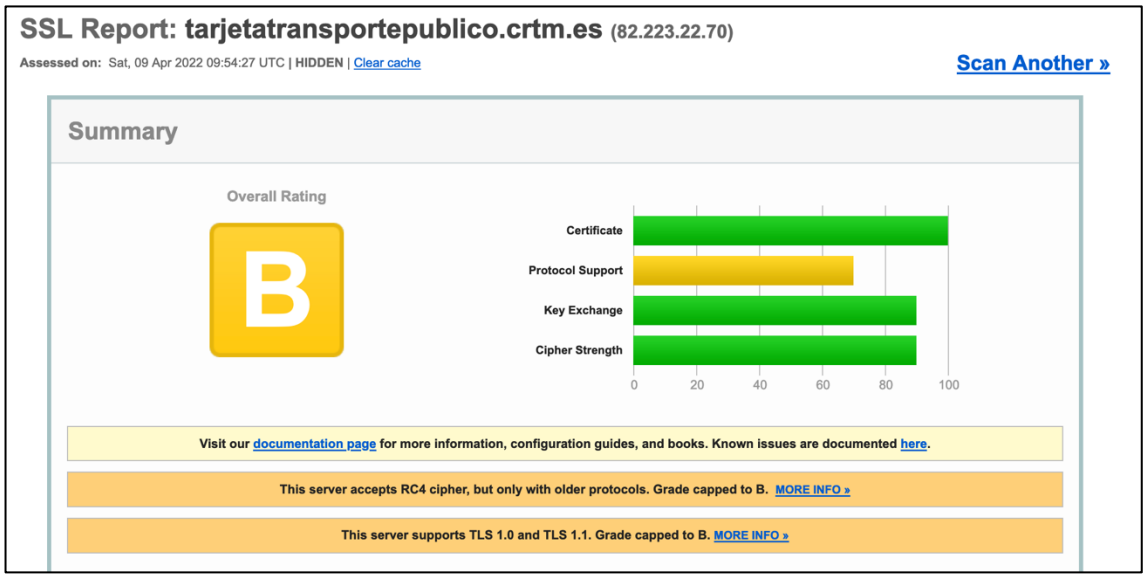


Figure 48. CRTM's website overall security rating by Qualys SSL test

In terms of protocols, we can see that it supports TLS 1.0, 1.1 and 1.2. Additionally, the site does not support SSL 2 and 3 which are completely broken (102)

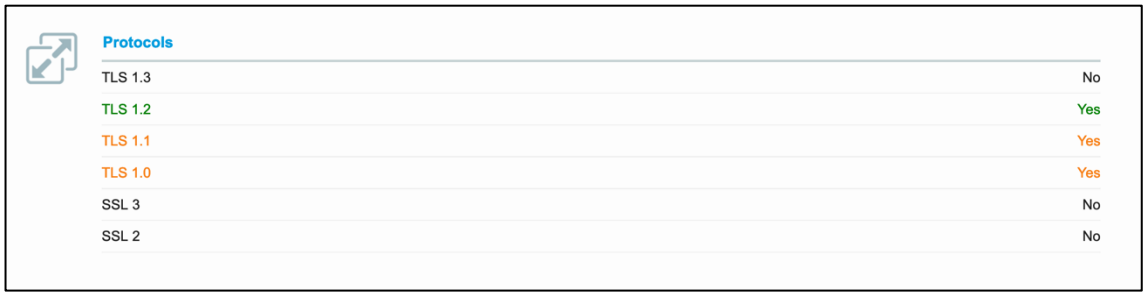


Figure 49. CRTM's website protocols supported

Figures 50, 51, and 52, show the cipher suites supported for TLS 1.2, 1.1, and 1.0 respectively. As we can see, even though TLS 1.2 is the recommended version, it also has ciphers that are not recommended due to being considered weak, and as such, recommended ones should be used.

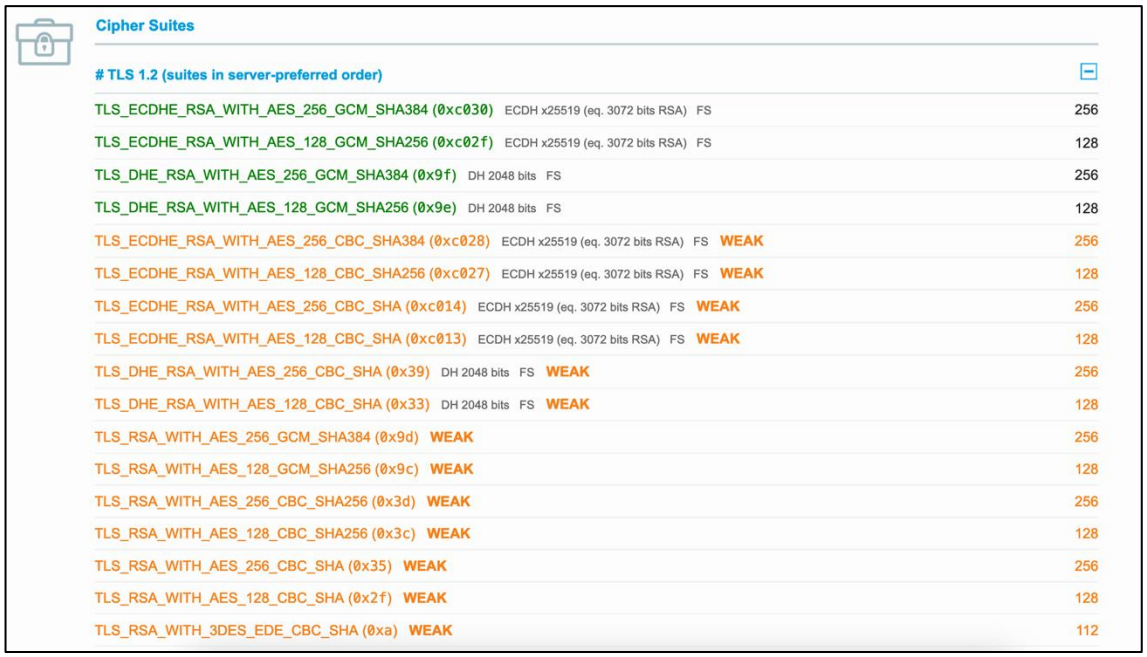


Figure 50. CRTM's website TLS 1.2 cipher suites

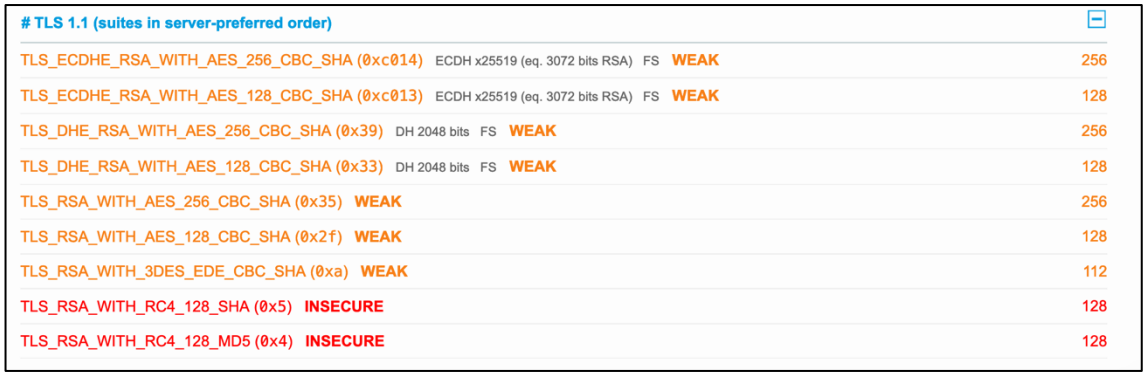
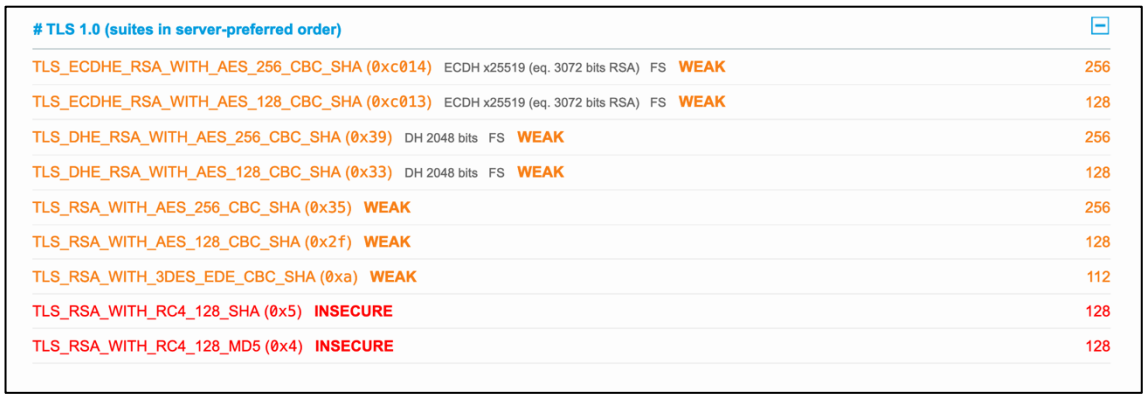


Figure 51. CRTM's website TLS 1.1 cipher suites

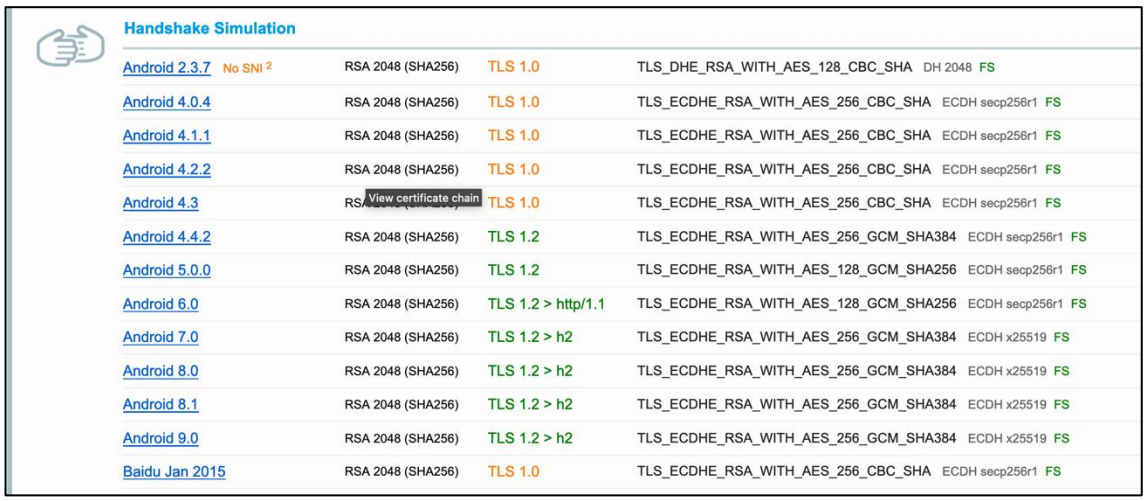


# TLS 1.0 (suites in server-preferred order)		
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	**WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	**WEAK**	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	**WEAK**	112
TLS_RSA_WITH_RC4_128_SHA (0x5)	**INSECURE**	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	**INSECURE**	128

Figure 52. CRTM's website TLS 1.0 cipher suites

Even though the use of TLS 1.0 and 1.1 is not recommended, it can be still used to increment the range of devices that can access your website. That is, supporting legacy devices. This makes sense if we observe the Handshake simulation performed by the Qualys tool where it emulates connecting to the website from different devices and operative systems.

As we can see, most modern devices connect through TLS 1.2 with ease but there are still a few of them, particularly old operative systems that do not support modern TLS versions and as such only connect thru TLS 1.0



Handshake Simulation			
Android 2.3.7 No SNI 2	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.3	View certificate chain	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS

Figure 53. CRTM's website handshake simulation results

Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 8 / XP No FS 1 No SNI 2	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 2048 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 2048 FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 2048 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

Figure 54. CRTM's website handshake simulation Cont.

6.8) Security Concerns

6.8.1) Phishing

One of the most prevalent cybersecurity attacks today that relies on people's naivety is phishing attacks. These attacks exploit the weakest link, human trust, social interaction, and lack of awareness. If a user is successfully tricked into willingly providing sensitive information to bad actors such as credentials, bank details, or simply clicking on a link, it could unchain serious consequences.

For instance, personal details could be used for impersonation purposes and ID theft. Clicking on a seemingly unoffensive link or attached document could lead users to perform automated actions on websites, from downloading and installing malware to bank transfers. For this last action mentioned, phishing is chained with XSS and CSRF attacks on vulnerable sites for further impact.

In theory, every website with a login portal is susceptible to phishing attacks, although certain technical safeguards can be implemented to enhance user security and prevent fraud. Multi-factor authentication is a good way to prevent this so that if the user's credentials are compromised, the attacker would still need access to go through the second factor. This second factor can be an app installed on the user's smartphone that prompts a code, or a login notification the user must approve.

In the context of CRTM's passengers, after browsing TTP website https://tarjetatransportepublico.crtm.es/CRTM-ABONOS/home.aspx a login page for users was not found. CRTM's website does not provide this feature and as such, users could simply not have an account within them. Therefore, the likelihood and impact of phishing attacks that directly impact a user account are non-existent. There is, however, a risk of general phishing by attempting to impersonate CRTM, EMT, or Renfe, thus gaining personal or bank details.

6.8.2) Privacy

In the event of theft or loss of the TTP card, the user's privacy is impacted as the cardholder's data is printed on the front of the card. Thus, anyone with visual access to it will see the name, surname, and passport photograph. As the card has a unique ID associated with the user's identity, its travel patterns and

This risk is not present in the general version of the card as no personal information is collected when issued.

6.8.3) Distributed Denial of Service (DDoS)

DDoS attacks consist in sending massive amounts of traffic to a single site through coordinated devices to impact the availability of a service. In the context of Madrid's public transportation and smartcards, CTRM's website unavailability would cause future passengers to be prevented from registering and requesting a TTP card.

We previously mentioned the existence of an app that allows users to top up their cards through their smartphones. To complete this operation, the app communicates with CTRM's endpoints in the ctrm.es domain through API calls (103). Therefore, if a DDoS attack disrupts those endpoints, users will not be able to top up or check their balances.

It is unknown whether a DDoS attack would also affect the infrastructure and network supporting CRTM's vending machines and smartcards top ups through them as the process behind it, traffic flows, and endpoints it might contact are unknown.

6.8.4) Paper Tickets

CRTM does not use paper tickets for granting access to their network. Only valid alternatives are either the general or personalized version of the smartcard or a contactless smart device for EMT buses. Therefore, the potential attacks previously discussed on paper tickets are not feasible in this context.

6.8.5) Contactless mobile and bank payments

CRTM's metro network can only be accessed with a valid CRTM's smartcard. In addition to this card, EMT buses fare can also be paid through smart devices and contactless bank cards via NFC technology. Passengers only need to tap their smart device such as a mobile phone or wearable associated with a bank card in a digital wallet or directly tap their physical contactless bank card.

The concern at this point might be the presence of a rogue terminal installed on EMT fleet that might charge an incorrect amount to users or attempt to steal their bank card information. However, the feasibility of this attack is unlikely as this would mean an unauthorized individual must have physical access to the bus and then the technical expertise to unmount the official terminal and install the rogue one.

6.8.6) Side-channel attacks

As it has been previously mentioned, CTRM's smartcard uses MIFARE DESFire EV1 technology. As of now, there are no known side-channel attacks capable of impacting this technology. There are, however, successful attacks on its previous version, MIFARE DESFire, through power analysis and templates by which the key can be cracked (104)

6.8.7) Man-in-the-Middle (MITM)

Man-in-the-Middle attack occurs when an unauthorized individual eavesdrops on a conversation between two parties. The malicious individual can gain access to confidential information should the channel not be encrypted and can even alter the message being transmitted.

In the context of CRTM's network, MITM could be conducted on three main points:

1. Between a user and CRTM's website
2. Between the smartphone app and CRTM API
3. Between the transport smartcard and the terminal

If MITM is successful at point 1), a malicious entity could obtain personal details of the user such as name, surname, photograph, home address, and national ID number. It could also obtain bank card information when the user is prompted to pay the fee to request the TTP card. This would be successful should the communication be in plaintext through HTTP. However, the site uses a valid certificate that allows establishing a secure HTTPS connection through TLS 1.2. If the communication remains through TLS 1.2 with a strong cipher it can be considered secure, although the page also supports TLS 1.1 and TLS 1.0 for compatibility purposes that could cause a risk should a downgrade attacks happen

Should a MITM attack occur at point 2), an attacker could also obtain bank card information and interfere with users' top ups. To protect against this attack at this point, HTTPS is also used as can be seen in figure 55. This figure depicts the message obtained when navigating to CRTM's API endpoints indicating SSL is enabled and therefore, HTTPS should be used.

The last point considered for a potential MITM attack would be 3) which would imply eavesdropping on the NFC communication. The available safeguard to protect against this attack is the mutual authentication process that occurs between the terminal and the card. Both components prove to each other that they pose the same encrypted key thus allowing them to trust each other. Through this secret key, a unique session key is generated per session to secure the communication.

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Reason: You're speaking plain HTTP to an SSL-enabled server port.<br />
Instead use the HTTPS scheme to access this URL, please.<br />
<blockquote>Hint: <a href="https://lat1p.crtm.es/"><b>https://lat1p.crtm.es/</b></a></blockquote></p>
<hr>
<address>Apache/2.2.3 (CentOS) Server at lat1p.crtm.es Port 443</address>
</body></html>
```

Figure 55. CRTM's API endpoint message

6.8.8) Unofficial apps

The last vector that could represent a threat to the security of CRTM's network is a look-alike unofficial version of the official CRTM app. In this context, users could download a malicious app believing it would help them to interact with their transport cards, but they end up giving up personal information or bank information inadvertently.

This vector is tricker to counter as it could be seen as a subset of social engineering where users are tricked to download and use a malicious app. The best safeguards against this are awareness campaigns and indicating to users how to get the official apps through official CRTM channels.

Chapter 7: Cryptographic protocols

This section covers the most relevant cryptographic protocols used in smart ticketing systems as well as lightweight ciphers aimed for IoT, smart cities, and constrained devices.

A summary of the cryptographic protocols relevant to this work is included in Table 4 below.

Table 4. Cryptographic protocols summary

Algorithm	Type	Operation	Advantages	Disadvantages
DES	Traditional	Block	Faster than 3DES	Not considered secure anymore Vulnerable to bruteforce attacks
3DES	Traditional	Block	More secure than DES	Weak About to be deprecated and disallowed
AES	Traditional	Block	Robust Strong Fast	Not entirely suitable for constrained devices due to resource consumption.
Crypto-1	Traditional	Stream	-	Weaknesses found
PRESENT	Lightweight	Block	Works on ultra constrained devices Less memory and power consumption than AES	High-power consumption
CLEFIA	Lightweight	Block	Long keys and block length	Implementation bigger than 2000 GE
Enocoro	Lightweight	Stream	Low power consumption	Security concerns in its 128v1
TRIVIUM	Lightweight	Stream	High trouhput Small area	Hardware implementation is costly Security concerns

7.1) Standard cryptographic protocols

The following ciphers have been observed in the smartcards schemes and ticketing systems reviewed:

7.1.1) Data Encryption Standard (DES)

DES is one of the first algorithms developed to protect the confidentiality of data and was accepted as an encryption standard in the US in 1976. It is classified as a block cipher with a size of 64-bits per block and a symmetric algorithm as it uses a secret key to perform both decryption and encryption. If a block were smaller than 64-bit, padding techniques are used by which bits are added to the block until it reaches the required length.

DES counts with three different operation modes namely Electronic Code Book (ECB), Chain Block Coding (CBC), and Cipher Feedback (CFB). The first one involves encrypting and decryption each 64-bit block independently, thus having no dependencies. However, its use is not recommended anymore. CBC and CFB do have dependencies. In the former, an Initialization Vector (IV) is used, and each 64-bit block depends on the previous one whereas the latter has dependencies with the previous ciphertext which by it becomes the input for the encryption operation. The result of this operation produces a pseudorandom output which was generated using XOR with plaintext.

In a nutshell, DES takes a plaintext block of 64-bit size and returns a ciphertext of the same size. The transformation from plaintext and ciphertext occurs through permutations of 2^{64} possible combinations of 64-bit where values can be either 0 or 1. DES performs an initial permutation followed by 16 operation rounds and a final permutation.

The cipher works as follows (105) :

1. The algorithm takes a 64-bit plaintext block
2. This block is given to an initial permutation function
3. This permutation splits the permuted plaintext in half, thus having a Left Plaintext (LPT) and Right Plaintext (RPT)
4. Each part goes under 16 rounds of encryption
5. Both parts are now joined back together and a final permutation is performed
6. This final permutation results in the 64-bit final ciphertext.

The problem with DES concerns the length of the secret key. This is 64-bit although, it is only 56 bits as every 8^{th} bit of the key are considered as parity bits, used to check for errors in the ciphertext. This short key leaves the cipher vulnerable to brute force attacks. Due to this, DES algorithm is not considered secure anymore.

Even though the use of DES was observed in the ticketing systems reviewed, the recommendation is to avoid it due to its weaknesses.

7.1.2) Triple Data Encryption Standard (3DES)

3DES was first published in 1981 in response to the weaknesses found in DES. This cipher applies DES algorithm three times to each block, thus encrypting data three times. These three runs are done with three 56-bit keys in which the DES process is applied in each run. Let's call them K_1, K_2, and K_3. K_1 is used in the first run to encrypt the plaintext. The resulting ciphertext is used by K_2 to perform a decrypt operation whose result serves as input for the last encryption operation performed by K (106). This is better shown in the following equation where E denotes encryption and D denotes decryption operation.

$$ciphertext = E_{K3}(D_{K2}(E_{K1}(plaintext)))$$

There are three possible combinations regarding the keys, these are:

1. The three keys are the same. This is the most vulnerable alternative as it was done for compatibility purposes with DES. In this situation K_1=K_2= K_3
2. The three keys are different. This is the strongest alternative as each key is a separate 56-bit key therefore having 3 * 56 = 168 separated key bits.
3. Two keys are independent (K_1 and K_2) and K_3 = K_1. The key length of this option is shortened to 2 * 56 = 112 separated key bits.

The security of the 3DES cipher varies depending on the alternative selected for its keys. Alternative 1 outlined above would be equal to simply using DES, and as such, its security is broken as mentioned previously. Option 2 provides a secret key of 168 bit which in reality is reduced to 112 bits due to meet-in-the-middle attacks, which is a technique useful against algorithms that repeats their operations several times. Option 3 provides better security than option 1 although it also leaves the key to 112-bit which is susceptible to attacks. Therefore, options 1 and 3 should not be implemented.

The use of 3DES was observed in the ticketing schemes reviewed. It was unclear as to which keying implementation these schemes used but considering option 1, and 3 listed above are deprecated or for legacy use, it would be thought option 2 is implemented. In any case, even when option 2 is implemented, the recommendation is to move away from 3DES as it will be considered deprecated in 2023 and disallowed after 2023 in favour of more secure algorithms such as AES or XChaCha20.

7.1.3) Advanced Encryption Standard (AES)

AES is one of the most popular encryption algorithms nowadays thanks to its reliability and security. It is the defacto cipher standard in the U.S. AES is implemented in a wide variety of applications thanks to its proven effectiveness when it comes to protecting the confidentiality of sensitive information.

AES is a symmetric block cipher that started development in 1997 in response to the weaknesses found in DES. Instead of the 64-bit block DES and 3DES use, AES uses a 128-bit block size of plaintext/ciphertext for both encryption and decryption

operations respectively. The secret key length was also incremented to 128, 192, and 256 bits.

It can be implemented in both hardware and software and it offers robustness and speed in them. The cipher is open source so it is available for anyone to implement. When compared to DES and 3DES, AES offers a higher security protection thanks to a longer key length than DES and 3DES.

Longer keys imply higher security although it might take a toll in terms of performance. Therefore a balance between security and performance is needed specially for the fast transactions required in ticketing systems. In the ticketing schemes reviewed, we found a common point of supporting AES with a key of 128-bit.

As of now, there are no successful known attacks against AES. Therefore, it is a suitable candidate to protect the confidentiality of ticketing systems and passengers' data. We have seen in the schemes reviewed the use of AES, especially for the modern version of MIFARE DESFire family, the CIPURSE and CEPAS standard, and the use in the FeliCA scheme. The common point is the use of AES with a 128-bit key.

7.1.4) Crypto-1

Crypto-1 was observed in the implementation of MIFARE technology as it is a proprietary protocol developed by NXP Semiconductors. As a proprietary protocol, its functioning remained secret until it was reversed engineered in 2009. Needless to say that from this point onwards the cipher was considered insecure and even when a newer version was created by NXP, it was also cracked. Therefore, the recommendation is to move away from this protocol and shift towards AES.

Contrary to the protocols mentioned above, Crypto-1 is a symmetric stream cipher having a 48-bit linear feedback shift register that controls the state of the cipher. The initial state is a secret and although it uses three Boolean functions that take 20 bits from the linear feedback shift register and produce 1 bit which is used to generate the keystream.

7.2) Lightweight cryptographic protocols

Even though it was found that the schemes and systems reviewed in this work do not use lightweight ciphers in their implementations, it was decided to comment on the most promising lightweight ciphers that could be implemented in the future in the context of smart cities and smart transportation.

NIST considers an 80-bit key length to be the minimum for lightweight cryptography. For enhanced security, 112-bit and longer are recommended. Also, according to ISO/IEC standardization, a lightweight cipher should have a Gate Equivalent (GE) value between 1000 and 2000.

7.2.1) PRESENT

PRESENT was created in 2007 in response to the need for fast and light ciphers to work in constrained environments. It is a symmetric block cipher with a block size of 64-bit, key size of either 80 or 128 bits, it counts with 31 rounds, and it is based on an SP-network. It's open source and it was designed to be used in devices that require low-power consumption and high efficiency.

In terms of functioning, each of the 31 rounds performs the following operations:

1. **addRoundKey**
   It performs a XOR operation on the output coming from the previous round, or the plaintext if it is the first round with the round key. The round key is generated by the Key schedule and it actually reduces the secret key length. For instance, if 80 bit implementation is used, the key would be reduced from 80-bit to 64-bit.

2. **sBoxLayer**
   PRESENT uses a S-box of 4-bit blocks. This operation takes the output from addRoundKey operation, put it in these 4-bit blocks and then performs 16 runs of this S-box.

3. **pLayer**
   The final step of each round involves taking the output of the sBoxLayer and performing a bit permutation based on a predefined table.

Once the rounds are complete, the last step of the cipher involves performing another XOR operation to the output of the rounds. In this XOR operation, a round key is used. (107)

Regarding its performance, the work "*Comparison of AES and PRESENT Block Cipher for 6LoWPAN Based Internet of Things"* (108) compared the performance between AES and PRESENT and showed that PRESENT consumes less memory and computation time than AES. One of the most outstanding implementations of PRESENT only uses around 1000 GE. Its main drawback is the high-energy consumption, and that security concerns arise through side-channel attacks, biclique cryptanalysis, etc. (109)

In terms of standardization, ISO included PRESENT in the ISO/IEC 29192-2:2019 specification for applications that require lightweight cryptographic implementations.

7.2.2) CLEFIA

CLEFIA is a symmetric lightweight cipher with a block size of 128-bit and key size of either 128, 192, and 256 bits. It was developed by SONY and it uses 18, 22, and 26 rounds depending of the key length. The cipher is outstandingly efficient in both software and hardware implementations. (109)

CLEFIA is alongside PRESENT another standardized block cipher for lightweight cryptography. It was also included in the ISO/IEC 29192-2:2019 specification for applications that require lightweight cryptographic implementations.

Its most ultra-lightweight implementation occurs 2488 GE only encryption. If both operations are desired, the number of GE increases to 2604GE (109)

7.2.3) Enocoro

Enocoro is a lightweight stream cipher that was standardized by ISO/IEC 29192-3. Two versions exists whose names depend on the key size they use, Enocoro-80 and Eonocoro-128, which use key sizes of 80 or 128 bits. The main advantage of Enocoro is its low power consumption.

It is worth noting that there exists two principal versions of Enocoro-128, v1 and v2. V1 was discontinued due to vulnerabilities discovered. In response to this, v2 was generated to address this issue using 64-bit as Initialization Vector.

7.2.4) Trivium

Trivium is a lightweight stream cipher standardized by ISO in the ISO/IEC 20192-3. It has a 80-bit key length and uses 80-bit length initialization vector (IV). It works by having three interconnected non-linear feedback shift registered with variable lengths, starting at 84-bit, passing through 93-bit, and finishing with 111-bit respectively.

The main disadvantages of Trivium are that its hardware implementation requires many flip flops, and that there have been publications about successful attacks against Trivium due to its simple design.

7.3) TLS cryptographic protocols

This section includes the recommended cryptographic protocols for protecting HTTPS communications. This is useful when the ticketing system infrastructure counts with a website and/or REST API.

Secure Socket Layer (SSL) is the predecessor of modern Transport Layer Security (TLS). These protocols were designed to protect communications between a client and a server through the use of encryption so that eavesdroppers could not view the message.

SSL is now deprecated due to security concerns and as such, versions 2.0 and 3.0 are considered insecure and should not be used. TLS came into play to address the

security vulnerabilities found in SSL. However, several attacks were found impacting TLS v1.0 and v.1.1 such as FREAK, POODLE, CRIME and BEAST attacks. The recommendation at this point is to move away from these TLS versions and only accept TLS v1.2 and higher. This however will impact the compatibility with legacy devices, thus impacting the overall number of users who can access these services.

Focusing on TLS 1.2, there are several recommended cipher suites for the vast majority of services. These cipher suites are composed of key exchange, authentication, bulk encryption, and mac/hashing algorithms. Table 5 below shows some examples of the recommended cipher suites (110) (111):

Table 5. TLS v1.2 recommended cipher suites

Key Exchange	Authentication	Bulk Encryption	MAC/Hashing
ECDHE	RSA	AES 256-GCM	SHA384
ECDHE	RSA	AES 128-GCM	SHA256
DHE	RSA	AES 256-GCM	SHA384
DHE	RSA	AES 128-GCM	SHA256
ECDHE	ECDSA	AES 128-GCM	SHA256
ECDHE	RSA	AES 128-GCM	SHA256

Chapter 8: Conclusions & Future work

In this work, we have examined the security controls around smart ticketing systems and their components to understand the potential security threats and privacy concerns they are exposed to. We have outlined the important role smart components play in granting access to transportation systems, especially smartcards. They are easy to use, convenient for both transport authorities and users, and fast. We have mentioned how their personalized versions have the implicit privacy risk of exposing cardholders' PII if they were stolen or lost.

Concerning smartcards standards and schemes, we have described both proprietary and public alternatives, being ticketing systems based on MIFARE or Calypso the most used schemes globally. Therefore, a special interest in research groups was put to evaluate their security. We have seen how older versions of MIFARE cards are no longer recommended due to security concerns related to the broken proprietary cipher Crypto-1. MIFARE DESFire EV1 is the one used in transport services in several of the most relevant cities around the world, which to date, is the most secure MIFARE card with no successful exploits.

In terms of the encryption techniques used to protect the data contained in smartcards alongside the communication between the reader and the card itself, we have seen the use of DES, 3DES, and AES. Particularly, smartcards establish a unique key for each session between the terminal to both authenticate the other device to ensure it is trusted and to protect further communication.

Of the three encryption ciphers mentioned above, it is recommended implementing AES and avoiding DES and 3DES ciphers due to weaknesses as well as them being deprecated & disallowed from 2023 onwards. Within AES, there are several key sizes that can be used. From the transport systems reviewed, it was observed the predominant use of 128-bit which offers a balance between performance and security as the longer the key, the more impact it has on its performance. Currently, the recommendation on this point is the implementation of AES-128 as the use of lightweight ciphers wasn't observed in the schemes reviewed.

Another critical point to apply safeguards to is applications users interact with. In the context reviewed in this work, these applications are transport authorities' websites through which users request and pay for issuing transport cards or log into their accounts, smartphone applications that allow to log in and view user's details as well as paying for services such as topping up transport smartcards, and REST APIs in which transport authority's servers are queried. The recommendation to secure the communication between clients and servers is to apply SSL/TLS certificates so that HTTPS connection is established. In addition to that, the suggested TLS version is 1.2 and higher with strong cipher suites such as:

- TLS_ECDHE_RSA_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_AES_128_GCM_SHA256

The principal risk users are exposed to, if a user dashboard behind an authentication portal exists in the system, is phishing. We have seen how phishing attempts to use social engineering techniques to exploit human behavior. Even though this type of attack cannot be successfully blocked entirely due to the nature of it (users will still be contacted via phone, email, or text messages), certain safeguards can be implemented.

The recommendation to thwart these attacks is to apply additional security verification on the logging process such as Multi Factor Authentication (MFA) so that users need to provide further details to log into their accounts. Evidently, this is not bulletproof as users could still be tricked by further social engineering to provide this additional authentication factor to the attacker. However, it will put another obstacle attackers would need to overcome to take over a user account, thus reducing the likelihood of occurrence.

Another risks these applications and overall infrastructure is exposed to are DDoS attacks that attempt to saturate the servers processing power with illegitimate requests. There are several protections that can be implemented depending on the architectural design. For simplicity's sake we will assume these applications are deployed on Cloud providers like Amazon Web Services (AWS) or Microsoft Azure. Cloud providers already provide free of charge DDoS protection through services like Shield in AWS. However, for enhanced security, the use of the advanced tier is recommended although this option incurs a cost. An additional and recommended security control that could be applied is a either cloud provider native or third-party Web Application Firewall (WAF) to protect website applications and REST APIs against Cross-Site Scripting (XSS) and SQL injection attacks.

With regards to limitations found during this work, we used information publicly available, therefore, accessing technical specifications behind a Non-Disclosure Agreement (NDA) was out of the scope. Another limitation was the unavailability of an Android smartphone with NFC technology which impacted our interaction with the CRTM's app, thus preventing us from examining its functioning, capabilities, and potential security and privacy concerns.

Last but not least, there are several ways this work can be further expanded and different paths to explore. One of them is performing an in-depth analysis of Madrid's TTP card to better understand its functioning at a low level. The protocols the card uses to communicate with an NFC terminal or CRTM's infrastructure could be analyzed. This could be achieved by using more specialized equipment that allows to debug NFC communications between the card and a reader connected to a computer.

Another path is to explore the CRTM's app on an Android device to evaluate its security, capabilities, overall functioning, and potential privacy concerns. Its APK could be debugged to identify traffic flows and the overall security implemented at a code level. During this exploration, another work could be conducted in parallel by analyzing

the NFC traffic between the card and the Android app when attempting to perform different operations such as reading remaining tickets, topping up the card, etc. In addition to this, the traffic between the app and CRTM's infrastructure could also be analyzed by setting up a proxy such as Burp Suite or Squid and making the smartphone route its traffic through it. In this way, HTTP traffic can be observed and analyzed to understand the traffic flows of these operations, endpoints, GET and POST requests and to also identify any weaknesses.

References

1. *The Internet of Things in Public Transport.* Brussels : International Association of Public Transport, 2020.

2. Internet of Things. [Online] Wikipedia, November 27, 2021. [Cited: November 27, 2021.] https://en.wikipedia.org/wiki/Internet_of_things.

3. Dunlap, Terry. The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History. [Online] IoT for all, June 20, 2020. [Cited: December 04, 2021.] https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities.

4. DDoS attack on Dyn. [Online] Wikipedia, November 6, 2021. [Cited: December 04, 2021.] https://en.wikipedia.org/wiki/DDoS_attack_on_Dyn.

5. Paul, Kari. [Online] The Guardian, December 23, 2020. [Cited: December 4, 2021.] https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats.

6. Mode of transportation. [Online] Saloodo, 2020. [Cited: November 20, 2021.] https://www.saloodo.com/logistics-dictionary/mode-of-transportation/.

7. Mode of transport. [Online] Wikipedia, November 18, 2021. [Cited: November 20, 2021.] https://en.wikipedia.org/wiki/Mode_of_transport.

8. Garg, Khushboo. Unimodal v. Multimodal Transportation of Goods. [Online] Legal Readings, June 29, 2021. [Cited: November 20, 2021.] https://legalreadings.com/unimodal-v-multimodal-transportation-of-goods/#Unimodal_Transport.

9. *Developing a user typology considering unimodal and intermodal mobility behavior: a cluster analysis approach using survey data.* Oostendorp, R., Nieland, S. & Gebhardt, L. 2019, European Transport Research .

10. Wireless, DDS. Here's Why Multi-Modal Transport is the Future of Travel. [Online] DDS Wireless, 2020. [Cited: December 07, 2021.] https://ddswireless.com/blog/heres-why-multi-modal-transport-is-the-future-of-travel/.

11. Rankil, W. *Smart Card Applications: Design models for using and programming smart.* s.l. : Wiley, 2007.

12. What is HCE? [Online] ClearBridge Mobile. [Cited: Feburary 28, 2022.] https://clearbridgemobile.com/what-is-hce/.

13. Developers Android. [Online] Google, October 27, 2021. [Cited: March 26, 2022.] https://developer.android.com/guide/topics/connectivity/nfc/hce.

14. Smart Cards in Healthcare FAQ Series – Smart Cards and Healthcare Providers. [Online] Secure Technology Alliance. [Cited: February 19, 2022.]

https://www.securetechalliance.org/publications-smart-card-technology-in-healthcare-series-smart-cards-and-healthcare-providers-faq/.

15. HSBC Bank Account. *HSBC.* [Online] HSBC, 2022. [Cited: February 19, 2022.] https://ciiom.hsbc.com/current-accounts/products/bank-account/.

16. Common Access Card (CAC). *DoD Common Access Card.* [Online] Department of Defense (DoD). [Cited: February 15, 2022.] https://www.cac.mil/common-access-card/.

17. University smart card: TUI. *Universidad Carlos III de Madrid.* [Online] Universidad Carlos III de Madrid, 2022. [Cited: February 19, 2022.] https://www.uc3m.es/life-on-campus/university-smart-card.

18. Northwest. [Online] Wikipedia, September 25, 2015. [Cited: February 19, 2022.] https://en.wikipedia.org/wiki/Compass_card_(British_Columbia)#/media/File:Cardplus Compasslogo.png.

19. Así funciona la Tarjeta sin Contacto. [Online] Renfe, January 11, 2021. [Cited: February 19, 2022.] https://blog.renfe.com/asi-funciona-la-tarjeta-sin-contacto/.

20. What is smart ticketing? *ITSO UK.* [Online] ITSO. [Cited: February 20, 2022.] https://www.itso.org.uk/about-us/what-is-smart-ticketing/.

21. Synopsis. Cryptography. *Synopsis.* [Online] Synopsys, 2022. [Cited: November 27, 2021.] https://www.synopsys.com/glossary/what-is-cryptography.html.

22. Forcepoint. The CIA Triad defined. [Online] Forcepoint, 2022. [Cited: December 07, 2021.] https://www.forcepoint.com/es/cyber-edu/cia-triad.

23. *Lightweight Cryptography for Internet of Insecure Things: A Survey,*. I. K. Dutta, B. Ghosh and M. Bayoumi. 2019. IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC).

24. *Lightweight cryptography methods.* William J. Buchanan, Shancang Li & Rameez Asif. 3-4, 2017, Journal of Cyber Security Technology, Vol. 1, pp. 187-201.

25. NIST. Lightweight cryptography. [Online] NIST, November 2, 2021. [Cited: November 2021, 27.] https://csrc.nist.gov/projects/lightweight-cryptography.

26. Kerry A. McKay, Larry Bassham,Meltem Sönmez Turan, Nicky Mouha. *Report on Lightweight Cryptography.* s.l. : NIST, 2017.

27. *Lightweight Cryptography for the Internet of Things.* Katagi, Masanobu & Moriai, Shiho. 2012.

28. Aleksandra Mileva, Vesna Dimitrova, Orhun Kara ,Miodrag J. Mihaljevic. Catalog and Illustrative Examples of Lightweight Cryptographic Primitives. *Security of Ubiquitous Computing.* 2021, pp. 21-47.

29. *Citations, Citation Indicators, and Research Quality: An Overview of Basic Concepts and Theories.* Dag W. Aksnes, Liv Langfeldt, Paul Wouters. 1, 2019, SAGE, Vol. 9.

30. *A survey of electronic ticketing applied to transport.* Macià Mut-Puigserver, M. Magdalena Payeras-Capellà, Josep-Lluís Ferrer-Gomila, Arnau Vives-Guasch, Jordi Castellà-Roca. 8, 2012, Computers & Security, Vol. 31, pp. 925-939.

31. *A Survey on Contactless Smart Cards and Payment System: Technologies, Policies, Attacks and Countermeasures.* Gupta, B.B., & Narayan, S. 2020, J. Glob. Inf. Manag., pp. 135-159.

32. *Eavesdropping near field communication.* Kortvedt, H., & Mjolsnes, S. NISK : s.n., 2009. The norwegian information security conference. p. 5768.

33. *Security in Near Field Communication (NFC). Strengths and weaknesses.* Ernst Haselsteiner, Klemens Breitfuß. 2006, In Workshop on RFID Security.

34. *All about encryption in smart card.* Montazerolzohour, M. Savari and M. 2012. 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec).

35. Smart Card Technology and Security. [Online] University of Chicago, 2000. [Cited: March 05, 2022.] https://people.cs.uchicago.edu/~dinoj/smartcard/security.html.

36. *Research on Encryption Technology in Contactless IC Card.* Zhao, Mingxin. s.l. : Atlantis Press, 2017. Proceedings of the 2017 7th International Conference on Applied Science, Engineering and Technology (ICASET 2017). pp. 256-259.

37. Sahula, T. K. Goyal and V. Lightweight security algorithm for low power IoT devices. *International Conference on Advances in Computing, Communications and Informatics (ICACCI).* 2016, pp. 1725-1729.

38. *A Survey on Symmetric Key Encryption Algorithms.* E. Surya, C.Diviya. 2022, International Journal of Computer Science & Communication Networks.

39. *A Survey on Lightweight Cryptographic Algorithms.* Sallam, Suzan. Jeju, Korea : s.n., 2018. TENCON 2018 - 2018 IEEE Region 10 Conference.

40. *Current Lightweight Cryptography Protocols in Smart City IoT Networks: A Survey.* . Rana, Muhammad & Mamun, Quazi & Islam, Rafiqul. 2020.

41. *Power efficient AES core for IoT constrained devices implemented in 130nm CMOS.* S. Agwa, E. Yahya and Y. Ismail. 2017, 017 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1-4.

42. M. Lu, A. Fan, J. Xu and W. Shan. A Compact, Lightweight and Low-Cost 8-Bit Datapath AES Circuit for IoT Applications in 28nm CMOS. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).* s.l. : IEEE, 2018, pp. 1464-1469.

43. *Overview of Security Threats for Smart Cards in the Public Transport Industry,.* K. Markantonakis, K. Mayes, D. Sauveron and I. G. Askoxylakis. 2008, 2008 IEEE International Conference on e-Business Engineering, pp. 506-513.

44. *"Power analysis attack: A vulnerability to smart card security.* H. J. Mahanta, A. K. Azad and A. K. Khan. 2015, 2015 International Conference on Signal Processing and Communication Engineering Systems, pp. 506-510.

45. *User Privacy in Transport Systems Based on RFID E-Tickets.* Sadeghi, A., Visconti, I., & Wachsmann, C. 2008, PiLBA.

46. *Lightweight cipher algorithms for smart cards security: A survey and open challenges.* J. Kaur, A. Kumar and M. Bansal. 2017. 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). pp. 541-546.

47. *Cryptographic algorithm optimisation.* Dhanuka, Suraj and Sachdeva, Priyam and Shaikh, Sharukh. 2015. pp. 1111-1116.

48. *Comparing and implementation of public key cryptography algorithms on smart card.* Zhang Peng, Jia Jian Fang. 2010. 2010 International Conference on Computer Application and System Modeling (ICCASM 2010). pp. 508-510.

49. *Privacy-Preserving Public Transport Ticketing System.* Milica Milutinovic, Koen Decroix, Vincent Naessens, Bart Decker. Fairfax, VA, United States : s.n., 2015. 29th IFIP Annual Conference on Data and Applications Security and Privacy (DBSEC),. pp. 135-150.

50. *Privacy-preserving billing for e-ticketing systems in public transportation.* Kerschbaum, Florian and Lim, Hoon and Gudymenko, Ivan. 2013. Proceedings of the ACM Conference on Computer and Communications Security. pp. 143-154.

51. Bus, First. First Bus App. *First Bus.* [Online] First Bus, 2022. [Cited: April 30, 2020.] https://www.firstbus.co.uk/tech-bus/first-bus-app.

52. Conger, Kate. Rare Malware Targeting Uber's Android App Uncovered. [Online] Gizmodo, March 01, 2018. [Cited: April 30, 2022.] https://gizmodo.com/rare-malware-targeting-ubers-android-app-uncovered-1821753862.

53. *QR Code Security.* Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, Edgar Weippl. 2010, SBA Research, pp. 8-10.

54. Waqas, Iam. Risks of Using QRCodes and How To Mitigate it – Not As Safe as You Think. [Online] IEEE Computer Society, October 19, 2021. [Cited: April 30, 2022.] https://www.computer.org/publications/tech-news/trends/qr-code-risks.

55. *Practical EMV Relay Protection* . Andreea-Ina Radu, Tom Chothia, Christopher J.P. Newton, Ioana Boureanu and Liqun Chen. 2022. 2022 IEEE Symposium on Security and Privacy.

56. *ISO/IEC 14443-1: Part 1: Physical characteristics.* s.l. : ISO.

57. ISO. *ISO/IEC 7810:2003.* 2003.

58. MIFARE Classic. [Online] NXP Semiconductors. [Cited: March 27, 2022.] https://www.mifare.net/en/products/chip-card-ics/mifare-classic/.

59. *Security Flaw in MIFARE Classic.* Ronny Wichers Schreur, Peter van Rossum, Flavio Garcia, Wouter Teepe, Jaap-Henk Hoepman, Bart Jacobs, Gerhard de Koning Gans, Roel Verdult, Ruben Muijrers, Ravindra Kali, and Vinesh Kali. 2008, Digital Security Group, Radboud University Nijmegen,.

60. *Dismantling mifare classic.* Garcia, Flavio & Gans, Gerhard & Muijrers, Ruben & van Rossum, Peter & Verdult, Roel & Schreur, Ronny & Jacobs, Bart. 5283, 2008, Lect. Note. Comput. Sci., pp. 97-114.

61. *Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards.* Carlo Meijer, and Roel Verdult. 2015, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security.

62. MIFARE PLus X. [Online] NXP Semiconductors, September 2018. [Cited: March 29, 2022.]

63. MIFARE Ultralight Family. [Online] NXP Semiconductors. [Cited: March 29, 2022.] https://www.mifare.net/en/products/chip-card-ics/mifare-ultralight/.

64. MetroMalaga. Metromalaga. [Online] Junta de Andalucia, 2022. [Cited: April 1, 2022.] https://metromalaga.es/billetes-y-tarifas/.

65. *Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World.* David Oswald, and Christof Paar. Nara : s.n., 2011. CHES 2011.

66. *Cloning Cryptographic RFID Cards for 25$.* Timo Kasper, Ingo von Maurich, David Oswald, Christof Paar. 2010, Horst Görtz Institute for IT Security.

67. SONY. FeliCa. [Online] Sony, 2022. [Cited: March 27, 2022.] https://www.sony.net/Products/felica/about/.

68. *Certification report Nº P165: Sony FeliCa Contactless Smart Card RC-S860.* Cheltenham : UK IT Security Evaluation and Certification Scheme, 2002.

69. ITSO. The national smart ticketing standard. [Online] ITSO limited. [Cited: March 26, 2022.] https://www.itso.org.uk/.

70. *CALYPSO FUNCTIONAL SPECIFICATION: Card Application.* s.l. : Calypso Networks Association, 2014.

71. CIPURSE Specifications. [Online] OSPT Alliance. [Cited: March 30, 2022.] https://www.osptalliance.org/cipurse-specifications/.

72. Octopus card. [Online] Wikipedia. [Cited: December 25, 2021.] https://en.wikipedia.org/wiki/Octopus_card.

73. Press Release. [Online] Octopus , October 17, 2017. [Cited: December 26, 2021.] https://www.octopus.com.hk/en/corporate/media/press-releases/2017/20171017.html.

74. *Security Analysis of the Octopus System.* Lee, A., Lui, T., & Leung, B.

75. Oyster. [Online] Transport For London. [Cited: December 08, 2021.] https://tfl.gov.uk/fares/how-to-pay-and-where-to-buy-tickets-and-oyster/pay-as-you-go/oyster-pay-as-you-go.

76. Nurmann, Frank. Tarjeta Oyster. [Online] Wikipedia, November 27, 2008. [Cited: December 27, 2021.] https://es.wikipedia.org/wiki/Oyster_card#/media/Archivo:Oystercard.jpg.

77. TfL to accept Apple Pay on public transport. [Online] Transport for London, June 8, 2015. [Cited: December 27, 2021.] https://tfl.gov.uk/info-for/media/press-releases/2015/june/tfl-to-accept-apple-pay-on-public-transport.

78. Android Pay accepted for pay as you go travel in London. [Online] Transport for London, May 18, 2016. [Cited: December 27, 2021.] https://tfl.gov.uk/info-for/media/press-releases/2016/may/android-pay-accepted-for-pay-as-you-go-travel-in-london.

79. Samsung Pay accepted for pay as you go travel in London. [Online] Transport for London, May 16, 2017. [Cited: December 27, 2021.] https://tfl.gov.uk/info-for/media/press-releases/2017/may/samsung-pay-accepted-for-pay-as-you-go-travel-in-london.

80. *Dismantling mifare classic*. Garcia, Flavio & Gans, Gerhard & Muijrers, Ruben & van Rossum, Peter & Verdult, Roel & Schreur, Ronny & Jacobs, Bart. Malaga : s.n., 2008, Lect. Note. Comput. Sci., Vol. 5283, pp. 97-114.

81. Suica. [Online] East Japan Railway Company. [Cited: December 27, 2021.] https://www.jreast.co.jp/e/pass/suica.html#category03.

82. Pay, Google. [Online] Google, May 23, 2018. [Cited: May 13, 2022.] https://blog.google/products/google-pay/add-suica-and-waon-google-pay-japan/.

83. EZ-Link Card. [Online] Viator. [Cited: December 28, 2021.] https://www.viator.com/es-ES/tours/Singapore/Ez-link-Card-Singapore/d18-57373P121.

84. CEPAS. [Online] Wikipedia. [Cited: December 28, 2021.] https://en.wikipedia.org/wiki/CEPAS.

85. Charms. [Online] EZ-Link. [Cited: December 28, 2021.] https://www.ezlink.com.sg/ez-charms/.

86. EZ-Link. [Online] Wikipedia. [Cited: December 28, 2021.] https://en.wikipedia.org/wiki/EZ-Link#Technical_data.

87. Wikipedia. [Online] October 1, 2019. [Cited: December 27, 2021.] https://commons.wikimedia.org/wiki/File:Carte_Navigo_2018_Verso.jpg.

88. Navigo Card. [Online] Île-de-France Mobilités. [Cited: December 27, 2021.] https://www.iledefrance-mobilites.fr/en/tickets-fares/detail/liberte-plus.

89. Calypso. [Online] January 8, 2021. [Cited: December 27, 2021.] https://calypsostandard.net/specifications/public-documents/87-010608-functional-card-application-v1-5.

90. MetroCard. [Online] Wikipedia. [Cited: December 28, 2021.] https://en.wikipedia.org/wiki/MetroCard#Future.

91. [Online] MTA. [Cited: December 28, 2021.] https://new.mta.info/.

92. About Contactless payments. [Online] Metropolitan Transportation Authority. [Cited: December 28, 2021.] https://omny.info/about-contactless-payments.

93. Opal. [Online] New South Wales Goverment. [Cited: December 28, 2021.] https://www.opal.com.au/ordercard/?execution=e1s1.

94. *The History of Transport Tickets in Madrid.* Madrid : Consorcio Regional de Transportes de Madrid, 2015.

95. MetroMadrid. Metro Madrid. [Online] 2022. https://www.metromadrid.es/en/travel-in-the-metro/card-types#panel0.

96. Metro Madrid. [Online] CTRM, August 14, 2021. [Cited: March 19, 2022.] https://www.metromadrid.es/es/nota-de-prensa/2021-08-14/la-comunidad-de-madrid-extiende-el-modelo-4-0-a-las-once-estaciones-de-metro-con-mayor-afluencia-de-viajeros.

97. Para, Kike. [Online] El País, January 29, 2020. [Cited: March 19, 2022.] https://elpais.com/ccaa/2020/01/29/madrid/1580298750_818668.html.

98. Así funciona la Tarjeta Sin Contacto. [Online] Renfe, January 11, 2021. [Cited: March 19, 2022.] https://blog.renfe.com/asi-funciona-la-tarjeta-sin-contacto/.

99. Paar, David Oswald and Christof. Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World. *Cryptographic Hardware and Embedded Systems.* Berlin : Springer Berlin Heidelberg., 2011, pp. 207–222.

100. Flynn, Rory. *An investigation of possible attacks on the MIFARE DESFire EV1 smartcard used in public transportation.* Dublin : Trinity College Dublin, 2021.

101. MetroMadrid. [Online] 2022. https://www.metromadrid.es/en/press-release/2020-03-01/the-regional-government-of-madrid-speeds-up-passenger-movements-in-the-madrid-underground-by-installing-quick-sale-ticket-machines.

102. Prodromou, Agathoklis. Acunetix. [Online] 2019. https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/.

103. mgp25, offk0rs, un1k0n. CTRM-NFC. [Online] March 18, 2020. [Cited: May 14, 2022.] https://github.com/CRTM-NFC/Mifare-Desfire.

104. *Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World.* David Oswald, Christof Paar. Nara : s.n., 2011. CHES.

105. Grabbe, J. Orlin. The DES Algorithm Illustrated. [Online] 2006. [Cited: May 18, 2022.] https://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm.

106. Lake, Josh. What is 3DES encryption and how does DES work? [Online] Comparitech, February 17, 2022. [Cited: May 18, 2022.] https://www.comparitech.com/blog/information-security/3des-encryption/.

107. *PRESENT: An Ultra-Lightweight Block Cipher.* Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. 2007.

108. *Comparison of AES and PRESENT Block Cipher for 6LoWPAN Based Internet-of-Things.* Thungon, Leki & Ahmed, Nurzaman & Hussain, Md. Iftekhar.parison of AES and PRESENT Block Cipher for 6LoWPAN Based Internet-of-Things. s.l. : International Journal of Computational Intelligence Systems, 2019, Vol. 1.

109. *A systematic review of ultra-lightweight encryption algorithms.* Noor Maher Naser, Jolan Rokan Naif. 1, s.l. : Int. J. Nonlinear Anal. Appl., 2022, Vol. 13.

110. Kiprin, Borislav. What are TLS/SSL Cipher Suites and how to order them. [Online] Cashtest Security, January 10, 2022. [Cited: May 25, 2022.] https://crashtest-security.com/configure-ssl-cipher-order/.

111. Muscat, Ian. Recommendations for TLS/SSL Cipher Hardening. [Online] Acunetix, April 10, 2019. [Cited: May 25, 2022.] https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/.

112. Cryptography. [Online] Wikipedia, November 1, 2021. [Cited: November 27, 2021.] https://en.wikipedia.org/wiki/Cryptography#Modern_cryptography.

113. Ticketing for multinodal. [Online] Thales. [Cited: December 04, 2021.] https://www.thalesgroup.com/en/markets/transport/fare-collection-management/seamless-travel-your-pocket/ticketing-multimodal.

114. Mobile Payments. [Online] Transit. [Cited: December 08, 2021.] https://transitapp.com/partners/payments.

115. Case Study: mobile ticketing. St. Catharines Transit Commission. [Online] [Cited: December 08, 2021.] https://transit.app/reports/mobile_ticketing_stcatharines_web.pdf.

116. [Online] Whim. [Cited: December 08, 2021.] https://whimapp.com/.

117. *Lightweight Cipher Algorithms for Smart Cards Security: A Survey and Open Challenges.* J. Kaur, A. Kumar and M. Bansal. Solan : s.n., 2017. 4th International Conference on Signal Processing, Computing and Control (ISPCC).

118. How do contactless smart transit cards work and are they secure? [Online] Thales. [Cited: December 19, 21.] https://justaskthales.com/en/how-do-contactless-smart-transit-cards-work-and-are-they-secure/.

119. Our Technology. [Online] Octopus Holdings Limited. [Cited: December 26, 2021.] https://www.octopus.com.hk/en/corporate/about-octopus/profile/technology/index.html.

120. Consorcio Regional de Transportes. [Online] 2019. [Cited: January 3, 2022.] https://www.crtm.es/atencion-al-cliente/area-de-descargas/publicaciones/historia-transporte-publico/breve-historia-de-los-billetes-del-ferrocarril-metropolitano-de-madrid-1919-2019.aspx.

121. Host-based Card Emulation. [Online] Google, October 27, 2021. [Cited: February 28, 2022.] https://developer.android.com/guide/topics/connectivity/nfc/hce.

122. Sean J. Barbeau, Jay Ligatti, Kevin Dennis, Maxat Alibayev. *Enhancing Cybersecurity in Public Transportation.* Tallahassee : Florida Department of Transportation, 2019.

123. ITSO Technical Specification. [Online] ITSO Ltd. [Cited: March 05, 2022.] https://www.itso.org.uk/services/itso-specification/itso-technical-specification/.

124. *A Comparative Survey on Symmetric Key Encryption Techniques.* Agrawal, Monika and Mishra, Pradeep. 2012, Int. J. Comput. Sci. Eng.