The security of mass transport ticketing systems

Marc Sel · Stefaan Seys · Eric Verheul

PricewaterhouseCoopers Enterprise Advisory Services
{marc.sel | stefaan.seys}@pwc.be
eric.verheul@pwc.nl

Abstract

Mass transport ticketing systems in most developed countries are making a rapid transition from 'traditional' paper or carton-based ticketing systems towards a contactless 'smart card' based approach. This article discusses the main IT security aspects of mass transport ticketing systems (metro, bus, etc).

We introduce the standards that emerged over the years, and we outline the core functionality of the IT aspects of a mass transport ticketing system.

We discuss some examples, and subsequently we address security and anti-fraud aspects. We also put some security breaches related to the use of the Philips/NXP Mifare family in perspective. We describe an alternative approach such as proposed by Calypso, and formulate conclusions and lessons learnt.

1 Introduction

1.1 Setting the scene

Mass transport systems in most developed countries are constantly evolving to offer better services for a better price. Organisations such as the UITP (International Association for Public Transport [UITP]) provide a global forum where operators promote ideas and turn them into reality. Over the last years, many operators are making a rapid transition from 'traditional' paper or carton-based ticketing systems towards a combination of contactless smart cards and cheap disposable tickets. These new technologies allow them to introduce flexible fare systems to better meet their clients' expectations, as well as to fight the increasing level of ticketing fraud. There are significant parallels with the credit card industry where an irreversible migration from magstrip to chip is taking place. This article discusses the security of such new ticketing systems.

1.2 About standards

Obviously, such systems have a long tradition, reflected in a number of existing standards. In 1998 the ISO 14443 Standard for Proximity Cards (13,56 MHz contactless interfacing) was published, including both -*A* (Mifare) and –*B* (RATP) variants. Today most readers support both variants, and most contactless systems rely on the standard for their radio interface.

Other influential standards include the EN 1545 Data Model family outlining the major data types, on which the ENV 12896 (Public Transport Data Model – [PTDM]) builds. This is further complemented

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2008), 1-10

by the EN 15320 (Interoperable Public Transport Application), and other models such as from the Calypso Network Association [CNA]. In 2004 the CEN TC278 WG3's 'Standard Architecture' was approved, and in 2007 the ISO 24014-1 Standard Architecture (Interoperable Fare Management System) was published.

Furthermore the CEN's CWA 14838 family describes EU policy and user requirements, provides guidance on smart card use, and outlines process requirements.

In some cases, standards may actually be competing, as in the case of the UK where London's Oyster followed another approach than the area outside London, governed by ITSO. Nevertheless, millions of users are served daily by cards such as Navigo (Paris), Mobib (Brussels), Oyster (London), OV-chipkaart (NL) etc. According to Eurosmart, a strong forum of leading smart card providers (see [Eurosmart]), some 170 million transport cards were shipped in 2007.

1.3 Functional aspects

A mass transport system allows people to travel from one place to another for a certain price, often subsidised. Mass transport operators offer a collection of possible fares. More often than not, the government's subsidising the system reflects the importance paid to the 'universal service' aspect of mass transport.

A passenger can purchase a contract in many forms (a single trip, multiple trips, season tickets etc.) at various points of sales. We use the term 'contract' to refer to the travel rights a passenger purchases. This contract can be stored either on a throw-away card or on a reusable, personalised or anonymous card.

When travelling, passengers have to demonstrate they are in possession of a valid contract. Most systems today are already (or are becoming) 'closed', i.e. a passenger needs to use his contract to enter the network. This is referred to as check-in. At the other end of the journey, the passenger has to perform a check-out. Intermediate validation may also be required, for example to calculate the optimal fare when switching transport mode. Individual verification by a controller only happens for a fraction of the passengers.

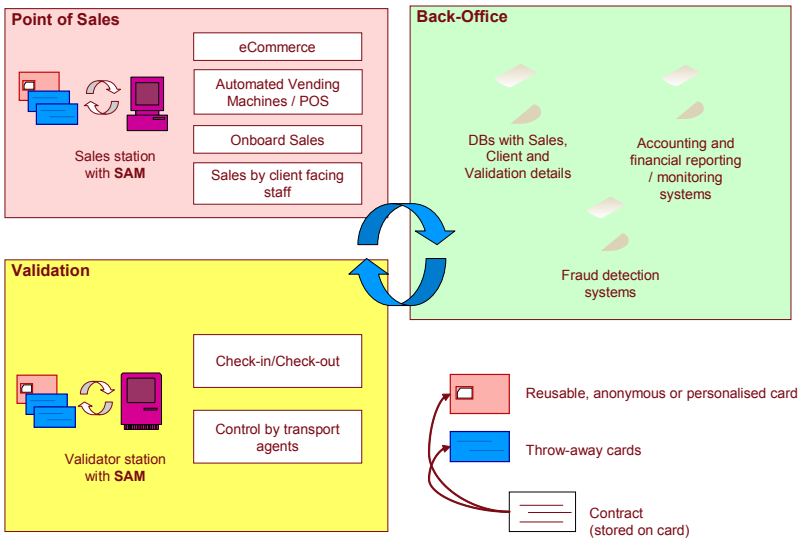

Figure 1: Components of a Mass Transport Ticketing system.

Figure 1 gives an overview of the most important functional components for a single operator system. The degree to which those components are connected on-line is an important feature of such a system. In a truly on-line system, the validator could check over the network whether a particular ticket is valid or not in a central database. However, since target time for performing a validation is 200 to 300 milliseconds, validation is a demanding process. Most systems download significant amounts of information to the validator, to speed-up processing and to cater for potential network problems.

1.4 Card issuance and personalisation

Different types of contactless cards are used. There is an obvious cost/capacity trade-off. Card memory typically ranges from ¼ K to 8K+ bytes. For example a 1K card handles usually maximum five contracts, a 4K card more than ten. What is particularly relevant here is that the card can store a history of previous journeys (but not necessarily a full journey log) which will influence the next fare to pay.

The first type is a cheap throw-away card that can be used for a single trip or for a certain amount of time (for example one day). We refer to these cards as 'tickets'. These tickets are issued with the contract already stored on the ticket. For single trip tickets, the contract on the ticket is flagged as 'used' at check-in (first validation) time, and subsequently cannot be used a second time. Tickets that are valid for a day will simply have an expiration time and will no longer be accepted when trying to validate them after this time. Sample cards include e.g. the Mifare Ultra-Light, which are priced around 0,20 to 0,5 euro for at least 100.000+ quantities.

The second type of cards is more expensive but can be recharged with different contracts. These cards have non-volatile rewritable memory that can be used to store any content that adheres to the data model specified for the card. These cards may be personalised for the passenger and contain the name, age and possibly other personal data, or they may be anonymous. These cards are issued at a point of sales at request of the passenger. If a passenger wishes, he can immediately purchase a contract that will be transmitted to the card (this will typically happen the first time a passenger purchases a monthly or yearly subscription). Sample cards include e.g. the Mifare Classic or DESFire, which may be priced around 1 euro or less for at least 100.000+ quantities. More expensive cards including Java cards typically cost less than around 5 euro.

To conduct his business, it is necessary for an operator to have an overview of all issued cards and tickets. Therefore, the IT system for card issuing has to maintain detailed records of all issued cards. The sales application will provide updates of all issued cards to a central database. The validators will upload details of the actions they performed as well.

1.5 Sales

Four main channels are commonly used to sell contracts to passengers:

1. Points of sales (POS) with client facing staff. Here, passengers can obtain a new card, new contracts, or stored value on their card. The sales application should be able to securely create new tickets or value, transfer it to the card and transfer all relevant transaction details to back office database systems.
2. Automated POS. This functionality is similar to the above, but usually only a subset of contracts can be purchased here (usually no monthly subscriptions). The security requirements are similar to the previous case.

3. eCommerce. Passengers purchase contracts over the Internet. The purchases are logged within the central databases at the back office and transferred to points of sales where the passengers can load their newly purchased contracts onto their cards. This may be possible at the validation points. The security requirements here are different: sales details have to be securely forwarded to all the points of sales (and validation points) and sales details have to be forwarded to the back office databases.
4. Sales onboard the vehicles. Some operators allow passengers to purchase contracts or tickets once they have boarded the vehicle. Usually the types of contracts that can be purchased here is limited. The security requirements are similar to the first two sales channels we discussed.

1.6 Contract validation

There are two main types of validation. The first type is performed by the passenger to ensure his ticket is valid. It is often implemented as the check-in/checkout to get the physical access to the transport network. The validating equipment needs to decide in milliseconds whether a valid contract is present in the list of current contracts, whether it has a new contract ready for download to the card, or whether it should decrease the stored value counter to pay for the check-in. And obviously, the black list needs to be verified as well. At positive outcome, the contract is marked as 'active' to prevent reuse and to allow agents to verify that passengers have actually validated their contract. The second type is validation by an agent. Here, agents will enter vehicles unexpected and verify that every passenger has a validated contract. Passengers without a valid contract will be fined. Usually, details of all validations are transferred to central databases stored within the back office of the operator.

1.7 Communication: Point of Sale to back office and vehicle to back office

Both sales and validation details have to be communicated to the back office databases. This can be straightforward when the points of sales have a fixed line to the back office, but more difficult when the validation happens on moving vehicles.

The technology used is depending on the environment and existing infrastructure. This can be a mix of wireless LAN standards, UMTS solutions, fibre back bones, etc. The transfer may take place in (near) real-time, or in batch.

1.8 Back Office control and monitoring

Back office control and monitoring is an important tool in the prevention of both internal and external fraud in any financial system. In mass transport ticketing systems, the back office will normally try to collect as much information as possible and permitted. This includes:

- Card issuing details: who has obtained which card at what time, who has delivered it, etc.
- Passenger history: all the card related actions (purchase, renewal, lost cards, etc.)
- Sales details: date, contract type, passenger ID, price, point of sales, etc.
- Validation details: date, location of validation, result of validation, etc.

It is obvious that there is a trade-off between the strength of controls and privacy. To respect privacy, it is recommended to at least segregate the databases into a database for basic customer information,

another database with more detailed attributes such as full address data, and a third database to log the transactions performed by the customer.

Using this data, the back office can build automated controls. The first type of control is performed by the sales department: reconciling expected income with the actual income. This control should happen on incremental levels: ranging from individual sales agents, over different sales channels, to overall checks.

The second type of controls is more specific to mass transport systems. Here the back office will build a number of checks that will detect 'unusual' behaviour. This can range from suspicious check-in/check-out sequences, suspicious timing of validation, suspicious locations of validations, etc.

As these controls rely on the completeness of the sales and validation details, the back office should also have sufficient controls to monitor the completeness of the related databases. These controls could include checksums on batches of data, verifying the number of transactions, etc.

Obviously these controls should be monitored and a dashboard should indicate potential fraud. Once fraud has been detected, corrective measure should be taken. The required action depends on the type of fraud: internal fraud may lead to discharging personnel, while external fraud will usually lead to black listing the card and possibly prosecuting the fraudster.

For types of fraud with little false positives, automated response could be used. Typical examples include the detection of card cloning. These cards can be automatically added to a black list without human intervention.

2 Two cases

2.1 The London Oyster

The London Oyster card serves as a relevant example of a contactless transport card. It is based on a Philips/NXP Mifare Classic card and allows travel on London transport (TfL – Transport for London), underground, DLR, National Rail and busses. According to the TfL website, the main contract was awarded in 1998 to the TranSys consortium for approximately 1.6 billion US dollar, for 17 years creation and operation of the system. The main card providers are SchlumbergerSema and G&D. The system was launched in 2003 with optional annual and monthly season tickets, and staff cards. Subsequently annual, monthly and weekly tickets were mandatory making use of the Oyster. Furthermore, 'Pay As You Go' was added, with possible auto-loading. The current Oyster allows a complex zone/time/age multi-modal fee structure but is nevertheless quite user friendly, with a daily price cap much appreciated by its users. According to TfL, in 2006, more than a billion (1014 million) journey stages were made via the London Underground. By March 2007, approximately two third of all underground journeys were made with Oyster. By 2009, compliance with ITSO standards (which are used in neighbouring transport systems) is intended. For more information refer to [TfL].

2.2 The Sydney Tcard failure

The Sydney Tcard serves an illustrative purpose of a larger scale failure. After 11 years and 95 million Australian dollars, the government called the program to a halt in January 2008. Sydney's public transport system is overseen by the NSW government, and includes State Transit, Sydney Ferries and CityRail. The main contractors were Integrated Transit Solutions Limited and ERG Group.

Various reasons have contributed to the overall failure, including the government demand to include multiple complex tariff schemes and 120 different CityRail ticket products for busses and ferries. Facing a potential 95 million dollar claim, ERG temporarily suffered a self-imposed trading halt on the Australian Stock Exchange. The project will go back to the drawing board. The NSW is reconsidering their options to revive the project as from the summer of 2008.

3 Security aspects

Basic requirements can be derived from use cases. Figure 2 show the most important use cases of a mass transport ticketing system.

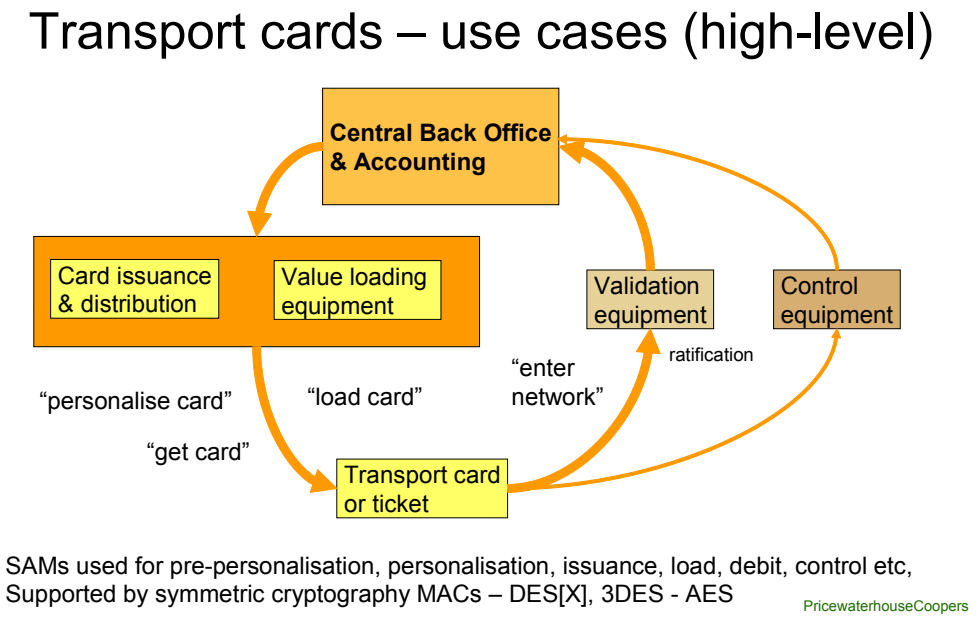

Figure 2: High-level Use Cases

The *first use case* is card personalisation. Depending on the type of personalisation chosen, the card may be anonymous, or may be a one-year season ticket for a particular student, or any other case.

The security properties depend on the type of card. Throw-away cards for single use generally do not have strong security capabilities. The cards may have a unique identity number that cannot be changed. They have 'write once read many' (WORM) memory cells to store the data. And there is a means to irreversibly write to the card, e.g. to indicate that the ticket has been used (e.g. by blowing a fuse on the chip). As there are no protected cryptographic secrets stored on the card, it is possible to clone these

cards. This is possible by intercepting the data they transmit and using it to emulate the card and the contract to a transponder.

Real chip cards have stronger security properties. These cards contain non-volatile memory with an authorisation mechanism. The card will only write to memory if the transponder can prove that it knows the correct cryptographic key. In turn, the transponder will only accept cards that can prove that they possess the appropriate key (using a challenge/response based protocol). The cryptographic keys used should not be exportable. If the cryptographic algorithm or its usage has weaknesses then keys can be recovered through cryptanalysis. Also the cryptographic algorithm should employ cryptographic keys of sufficient bitlength (entropy), to withstand brute force kind of attacks. Currently a symmetric keylength of 80 is considered the bare minimum, see [keylenght]. The proprietary Mifare Classic cryptographic algorithm (CRYPTO1) employs a 48 bit keylength which means that this algorithm became susceptible for brute force attacks as soon as the algorithm was known. However, it turned out that CRYPTO1 and its usage actually has weaknesses allowing for far more efficient attacks then brute force attacks.

The *second use case* is loading a contract on a card. This usually happens after the contract has been purchased. The cards will only respond to terminals that can prove knowledge of the correct cryptographic key. Such keys are stored within a Security Authentication Module (SAM). The transponder will use the functionality offered by the SAM to write data to the card. In a model based on symmetric keys, every card will normally have its own personal key that is derived from a master key and the unique identity of the card. The SAMs will all contain this master key, and a number of keys for the specific operations such as loading or validating. During the challenge/response protocol between the SAM and the card, the card will reveal its identity, which allows the SAM to compute the personal key of the card. This key is used for mutual authentication. Access control to the cards memory can be managed in the card data model (e.g., different SAMs can have access to different parts of the memory, some parts can be readable without authentication, etc.). These SAMs will be present in every piece of equipment that needs to write to the card (transponders at points of sales, validation stations, etc.). As these SAMs are dispersed at various public locations, it is important to protect them from theft. Next to physical theft protection, other measures need to be taken to prevent abuse of SAMs. Possible measures are limiting the number of times a SAM can be used. In this case, a 'master SAM' is used to set the ceilings in the other SAMs (using secure authentication). Other means are to store the ID of the SAM in every contract that it creates. This allows validation stations to consult a black list of stolen SAMs before validating a card.

The *third use case* is validating a contract. If the data stored on the card is readable for anyone, this will not require a SAM. The validation terminal will interrogate the card and verify that the contract is valid. If outcome of the validation has to be registered on the card, then a SAM is required to write this information to it.

The back office should be aware of all transactions related to cards and contracts. This means that all points of sales, validation stations and mobile terminals of patrolling agents have to be connected to the back office databases. The solution for these connections will be a composition of rather heterogeneous combinations of wireless connections, wired LAN, fibre back bones, UMTS, etc. As validation stations will be mounted on moving vehicles or carried around by patrolling agents, these connections will not be available at all times. This means that local caches of the gathered data are required. These caches can be pushed to the back office once a connection is available (for example in the bus depots). Obviously network layer security mechanisms have to be put in place to ensure that only authorised components have access to this heterogeneous network. These mechanism will typically be a mix of different technologies including PKI, VPNs, SSL connections and application layer security.

4 Mifare woes

NXP and its licensees market variants of the Mifare product family, for various purposes including mass transport systems. Two particularly relevant examples are the Mifare Ultralight, used as disposable ticket and the Mifare Classic used as anonymous or personalised card. Implementations include the London Oyster, and the Dutch national OV (Openbaar Vervoer = Public Transport) chipcard. Security weaknesses have recently been demonstrated for both the Ultralight and the Classic.

4.1 Mifare Ultralight problems

In the Netherlands, students of the University of Amsterdam evaluated the security of the disposable OV-chipcard, intended for a nation-wide roll-out. This card is based on the Mifare Ultralight. Such a card contains 512 bits of non-volatile storage, organised into a UID, lock bytes, OTP memory and a user area. The UID provides a unique identifier. The lock bytes contain bits that can force other bits into read-only mode. Executing such a lock cannot be reversed. The lock bytes also contain some block-locking bits which can prevent other lock bits from being activated. These bits can be used to prevent that information bits on a card can be locked. The OTP is a One Time Programmable counter, which is irreversible. It is used e.g. to keep track of the number of rides on a ticket. Finally the user area offers 48 bytes that are application specific. Here transaction data such as check-in/check-out as well as general information about the card (holder, issuer, contracts, etc) is stored.

Various attack scenarios were performed on the real system, leading to the conclusion that a single disposable ticket could be used for an almost unlimited number of trips, by backing-up and rewriting ticket data. No cryptographic knowledge or specialised hardware was required for this attack. The Dutch press was made aware of this in July 2007, and the implementer subsequently fixed the problem which was related to the usage made of the OTP counter by the reader. For the detailed report of Pieter Siekerman (from PricewaterhouseCoopers) and Maurits van der Schee refer to [vdS-S].

4.2 Mifare Classic problems

In December 2007, on the CCC ’07 conference, weaknesses in the CRYPTO1 proprietary and not disclosed algorithm were presented by Karsten Nohl and Henryk Plötz. They reverse-engineered the algorithm by analysing the physical implementation of the gates on the chip. They claim the algorithm is a linear feedback shift register algorithm with a 48 bit key. Given the current state of the art in computer hardware and crypt-analysis, 48 bits can be considered as too short.

In the Netherlands, TNO was invited to conduct evaluations by TLS, the OV-Chipcard operator. The outcome of these evaluations was subsequently released to the public (see [TNO-P]) and confirmed the problem.

This started further research, leading to the publication in March 2008 by Digital Security group of the Radboud University Nijmegen that they were able to crypt-analyse Mifare Classic keys in seconds. PricewaterhouseCoopers and Radbout University jointly performed an analysis of the use of the Mifare Classic as a nation-wide civil servant card for an EU Member State. While the details of this analysis remain at the discretion of this government, it is fair to state that our analysis confirmed the general line of thought that Mifare Classic can no longer be considered as secure in a number of usage scenarios. For more details please refer to [Radbout].

4.3 Way forward

NXP suggests the use of Mifare DESFire, Mifare Plus and SmartMX. Obviously, there is also a list of vendors with competitive products (Infineon, STM, etc). We recommend to consistently apply risk analysis to drive the overall price/quality decision.

5 An alternative approach

5.1 The Calypso approach

Calypso is proposed as a de-facto standard by the Calypso Network Association. It defines the interface between cards and terminals. The basis of the specification is 'Calypso Specification for Ticketing, Card Specification[1]', complemented by a set of 'Calypso Technical Notes[2]'. It relies on other well-known standards such as ISO 14443 et ISO 7816-1 – 3 for the radio link, ISO 7816-4 for APDU commands, and EN 1545 for the ticket/card data model. The components standardised are a Calypso-compliant smart-card, a disposable ticket, and a SAM (Secure Access Module). Main actors are CNA (Calypso Network Association), Innovatron (patentholder for some ISO 14443 et Calypso application patents (particularly « Session sécurisé et indivisible » and « ratification »), RATP (the Paris –based transport operator), and Spirtech.

The security of Calypso is to a great extend based on the use of diversified keys and MACs (message authentication codes). Cryptographically the security is based on DES, DESX and/or 3DES. Keys are managed in SAM hardware, with different keys being used for different functions (such as loading of a contract versus validation), and individually diversified keys. Apparently the use of AES has not yet been envisaged. The actual detailed security features of Calypso are not publicly available, and as such there is some 'security by obscurity' flavour present.

As Calypso is mainly focused on defining the interface between cards and terminals, various other aspects of a mass transport system such as an overall data model, and the application and back office aspects as well as interoperability with other fare systems still remain to be addressed outside the Calypso model.

5.2 Calypso implementations

There are many different ways of implementing a Calypso based system. Cards can be provided by some of the world's most respected names in smart card manufacturing. Applications and back office functions need to be developed to meet the specific requirements of the market. According to the Calypso Network Association, Calypso-based systems have been implemented in 21 countries, with more than 30 million contactless cards, relying on 300.000 terminals in some of the largest intermodal networks in the world such as Paris. Brussels is also currently migrating from magnetic-based system onto a Calypso implementation.

1 Document 010209-MU-CalypsoCardSpec
2 Documents CalypsoTN001 – TN014

6 Conclusion

Mass transport ticketing systems face universal problems with often quite tailor-made solutions that reflect the particular situation where the system operates. Adequate security should be considered a mandatory quality. The 'security by obscurity' approach of Mifare-based solutions can be considered as a thing of the past, and we recommend consistently avoiding this approach.

Good cryptography and security engineering are required as the foundation to build a performing, user-friendly and secure system. Such a system should contain comprehensive controls that span from card to accounting and financial systems, including the back-office.

References

[CCC07] Mifare Classic hack: Karsten Nohl, Starbug, HenrykPlötz, CCC report CCC '07, http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html

[CNA] Calypso Network Association - www.calypsonet-asso.org

[Eurosmart] Eurosmart – 'the voice of the smartcard industry' - www.eurosmart.com

[keylength] Refer to www.keylength.com

[PTDM] Public Transport Data Model - www.transmodel.org

[Radbout] Radbout University OV-chipcard wiki: https://ovchip.cs.ru.nl

[RFIDIOt] Adam Laurie's www.rfidiot.org library and website

[TfL] Transport for London, the London Oyster card: tfl.gov.uk

[TNO] TNO, 'Security Analysis of the Dutch OV-Chipkaart,' TNO report 34643, 2008. http://www.translink.nl/media/bijlagen/nieuws/TNO_ICT_-_Security_Analysis_OV-Chipkaart_-_public_report.pdf

[UITP] UITP – the International Association of Public Transport – www.uitp.org

[vdS-S] Mifare Ultralight hack report: http://staff.science.uva.nl/~delaat/sne-2006-2007/p41/report.pdf