TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur

State-of-the-Art Privacy Analysis of E-ticketing Systems

Work in progress

April 2012

Abstract

This essay performs state-of-the-art privacy analysis of e-ticketing systems taking into account both the proprietary solutions and respective standards developed so far.

1 Introduction

E-ticketing is a quite ambiguous notion and in this essay it is referred to as an alternative to the conventional way of proving the availability and validity of travel permission (e.g. paper tickets) through transferring the necessary information to an electronic medium (e.g. an RFID card). There is a plethora of solutions covering this issue that adhere to different concepts and utilize various technologies and standards (quite often proprietary). This essay is focused on *contactless smart cards* as the carrier medium of an e-ticket and therefore on the systems making use of this kind of cards and the respecting standards.

2 Advantages and Disadvantages of E-ticketing

2.1 Advantages

The e-ticket concept is attractive for both customers and service providers. From a *customer view*, it provides the following advantages:

- Faster and more convenient verification of a ticket [1];
- Saving on travel expenses due to the "pay-as-you-go" feature (paying for the actual distance travelled);
- The ability to profit from a flexible fare pricing scheme (with possible individual discounts and special offers);
- Revocation of lost tickets and their replacement [1];
- Increased usability:

– no need to have change for e.g. a local ticket issuing machine[1] (for instance, for customers only sporadically using the transport service or while being in another city);
– no need to carefully study complex fare pricing schemes: the system can automatically choose the best option and possibly suggest a discount (e.g. based on customer's travel habits);

For *public transport companies*, the adoption of the e-ticket concept can be beneficial due to the following reasons:

- Decrease in system maintenance costs [1, 2];
- Significant reduction of payment handling costs [3];
- Improvement of the fare dodgers rate through the more efficient ticket verification procedure [1];
- Mitigation of the ticket forgery problem (e.g. using suitable cryptographic primitives) [1];
- The ability to create highly flexible fare pricing schemes and innovative ticketing solutions [2];
- The opportunity to create innovative multi-application schemes combining transit with non-transit[2] functions [2];
- The possibility to create interoperable solutions between cooperating transport service providers with subsequent revenue sharing[3].
- Consequently, the ability to attract more customers and to generate more revenue.

2.2 Disadvantages

Along with tangible benefits, the concept of e-ticketing raises several concerns. For a *customer*, it is in the first turn privacy-related issues, namely:

- Ubiquitous customer identification;
- The possibility of customer profiling (creation of movement patterns, etc.);
- Resulting privacy violation through increased surveillance ("The Big Brother" problem).

For *transport companies*, moving to an e-ticketing system may raise the following concerns:

- Relatively high system development costs (no off-the-shelf, end-to-end solutions available);
- Lack of mature interoperable solutions and standardisation in the area as a whole (many of the developed e-ticketing systems are proprietary);
- The necessity to invest into a new infrastructure and deploy it (which might involve high risks for a relatively low-profit public transport business [2]);

[1]This is possible if an e-ticket is linked to a bank account of the customer. The latter can use his/her e-ticket in e.g. in another city without the necessity of buying for instance a single trip ticket from a local ticket issuing machine.

[2]For example, using an e-ticket for a discount in food vending machines deployed at stations, etc.

[3]The e-ticketing concept enables to create an interoperable architecture of public transport services from different transport companies (e.g. in different cities or even countries). This allows a customer to use a single e-ticket with different providers (*usability*) while the latter can share the profits from collaborative business relations.

- Possible reluctance to using the system from the customer side due to privacy reasons (raising privacy awareness and the necessity to invest in privacy to attract customers).
- To ensure interoperability between different service providers, the efficient, secure, and privacy-respecting sharing of the respective databases must be performed, which introduces yet another challenge to transport companies.

3 Privacy Concerns in RFID-based E-ticketing Systems

The following threats to the customer's privacy can be identified in RFID-based e-ticketing systems:

1. Unintended customer identification:
   (a) exposure of customer ID:
      i. personal ID exposure (direct identification),
      ii. indirect identification through the relevant object's ID[1] [4].
   (b) exposure of a non-encrypted identifier during the anti-collision session [5];
   (c) physical layer identification (RFID fingerprinting[2]).
2. Information linkage;
3. Illegal customer profiling.

Generally, the aforementioned threats should be considered together with the so-called *privacy protection goals* [7, 8]:

1. Anonymity;
2. Confidentiality;
3. Unlinkability;
4. Unobservability.

These high-level goals are supported by a set of generic privacy-preserving mechanisms, such as:

- Anonymization techniques (pseudonyms, etc.);
- Zero-knowledge proofs (e.g. during the authentication);
- Encryption of privacy-relevant information;
- Data minimization.

The application of these techniques to an RFID system and their efficient distribution across system components (in the front-end as well as in the back-end) is a research question and till now remains to a large extent open.

The results of a preliminary state-of-the-art study of countermeasures against the aforementioned privacy threats are listed in Table 1.

[1]The notion of object ID (OID) encompasses the following ID set: medium ID (unique card number), application ID (the unique identifier of an application instance installed on the card), etc. OID can therefore become an indirect personal identifier [4].

[2]For example, using the deviations of RFID chip backscatter frequency as a distinguishing factor, see [6].

Table 1: Privacy threats in RFID-based e-ticketing systems with respective countermeasures.

Threats	**Countermeasures**
1. Unintended customer identification:	
(a) Exposure of customer ID:	
i. personal ID exposure (direct)	Privacy-respecting authentication; ID encryption/randomization; access-control functions [9]
ii. indirect identification	ID encryption
(b) Unencrypted ID during anti-collision	Randomized bit encoding [10]; bit collision masking [11, 12] (protocol dependent)
(c) PHY-layer identification	Shielding; switchable antennas [13]
2. Information linkage	Anonymization (in front-end and back-end): threat 1 countermeasures; privacy-respecting data processing
3. Illegal customer profiling	Privacy-respecting data storage (back-end); the same as in threat 1

4 Existing Standards and Implementations

The architecture of an e-ticketing system can be coarsely divided into two main parts:

- *Front-end:* an RFID chip (the e-ticket carrier medium), an interface between the e-ticket carrier medium and the reading device (RFID reader) as well as an RFID reader itself;
- *Back-end:* an infrastructure with the necessary applications and databases.

In the front-end, the communication interface between the reader (terminal) and the RFID chip is already well standardised according to ISO14443 [14], which consists of 4 parts:

Part 1: Physical characteristics;

Part 2: Radio frequency interface power and signal interface;

Part 3: Initialization and anticollision;

Part 4: Transmission protocol.

Most of the current e-ticketing system implementations are based on this widely adopted standard. For example:

- Calypso e-ticketing system (Belgium, Canada, China, France, Israel, Italy, Portugal, etc.);
- E-ticketing systems based on MIFARE cards (Dutch OV-chipkaart, London's Oyster Card, Hong Kong's Octopus Card, the Puget Sound ORCA Card in the US, etc.).

In the back-end, however, the developed solutions may vary greatly. In order to enable full interoperability, a lot of effort has been targeted at the standardisation process. Figure 1 depicts the main standards developed so far spanning from the chip–reader interface up to the application layer.

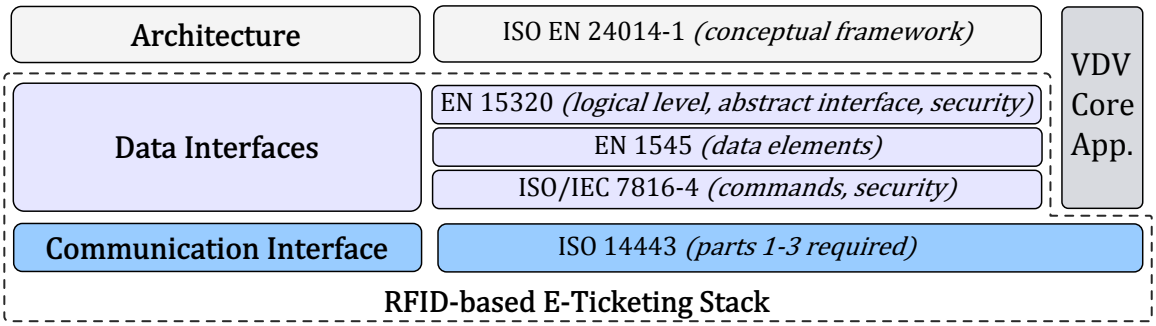

Figure 1: Standards supporting interoperable e-ticketing systems.

In order to bring the standards together and provide for a generic middleware system that can be used by different service providers, the solution named Core Application (Kernapplikation)[1] was created in Germany. According to the developers, it is generic enough to enable the interoperability (even across countries) between various e-ticketing systems which are based on it. Core Application was developed on top of the ISO14443 standard and is claimed to greatly improve the process of migrating from a set of proprietary solutions to a global one.

The interoperability goal implies the existence of common security and privacy measures (e.g. an agreement on mutually recognized and accepted security and privacy suits). The need for security is widely acknowledged by transport companies, since insecure solutions may result in substantial revenue losses (e.g. due to ticket forgery or system blackouts) and even lead to eventual phase-out of the system.

Privacy, namely customer privacy, to the contrary, is not in direct interest of service providers. The reason for this is that possible risks associated with privacy violation have far less serious implications for company business compared to security. However, the constantly rising privacy-awareness of customers and the ever growing likelihood of public outcry induced by the cases of privacy violation may stimulate transport companies to invest in privacy in order to remain competitive. The interoperability goal poses a further challenge to privacy since sharing of privacy-critical data, which is needed for a proper delivery of transport services by cooperating companies, should be performed in a privacy-preserving way.

5 E-ticketing: A General Application Scenario

The e-ticketing concept can be implemented in many different ways. The general application scenario, however, can be described as follows (see Figure 2). A customer purchases an e-ticket, possibly registering himself (i.e. disclosing his name and other information necessary for billing) to enable flexible pricing schemes with individual discounts. The trip begins when the customer enters the transport vehicle and checks in. The check-in procedure is performed through the reading device (reader) installed in the vehicle. The reader forwards the e-ticket ID (u_ID) to the on-board ID processing unit which registers the check-in time and the geographical coordinates[2]. When the customer has reached the final destination, he/she checks out (using the on-board reader) and leaves the transport vehi-

[1] http://www.vdv.de/wir_ueber_uns/vdv_projekte/vdv_kernapplikation_efm.html

[2] The coordinates determination can be performed through the GPS technology or, for example, registering the stop where a customer entered the transport vehicle. The combined approached is used in a so-called Vehicle Location System (VLS) which was deployed in Singapore public transport system [15].

cle. The time and the geographical coordinates are registered again and a "trip tuple" is eventually formed: $[u\_ID, vehicle\_ID, \text{in}(time, coordin.), \text{out}(time, coordin.)]$. The latter is then communicated to the back-end system to enable distance calculation with possible creation of individual fare pricing schemes and the respective billing procedure. All interchanges performed by the customer during the trip are therefore registered, respectively processed and billed.

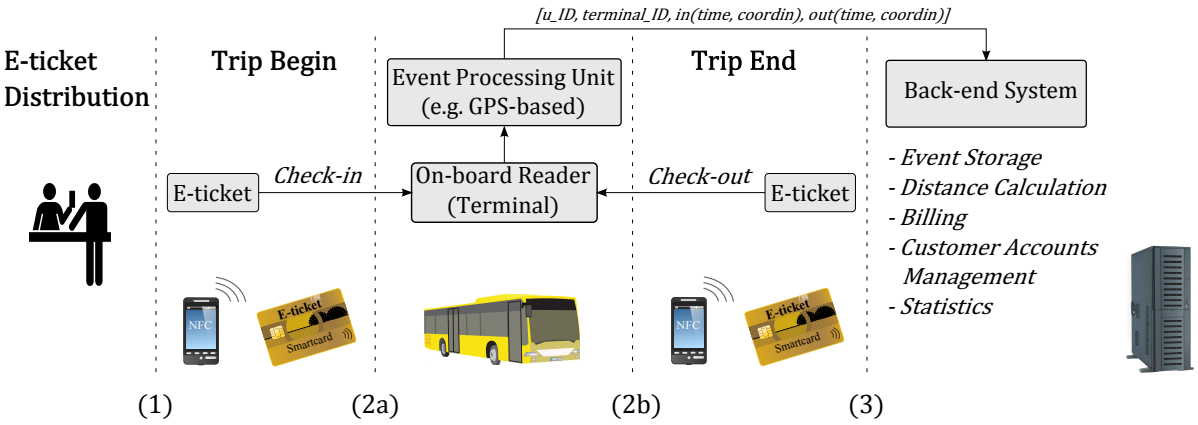

Figure 2: E-ticketing: a general application scenario.

Check-in/check-out can be carried out in an explicit or an implicit (seamless) way. The first one is referred to as the classic check-in/check-out (CICO) procedure when the customer has to hold an e-ticket for a certain amount of time in the vicinity of a reader to validate the ticket. If this is performed automatically on entering the vehicle without human intervention (implicitly), it is called be-in/be-out (BIBO). In this case, the RFID-chip in the e-ticket has to be active[1] (i.e. possessing its own power source) in order to enable seamless interaction with the reader.

6 E-ticketing: Privacy Issues Considered in the Respective Standards

The standards stack depicted in Figure 1 represents a generic structure of an e-ticketing system. In this section, a concise assessment of privacy and security measures specified in the respective standards is performed and presented in a "top-down" way. Various proprietary privacy solutions with respect to privacy are not considered in this section.

6.1 Architecture Layer

ISO EN 24014-1 The standard introduces a conceptual framework for developing an interoperable architecture for transport fare management systems. It describes the structure of an interoperable platform, its main actors, and general flows of information exchange. Privacy is considered at a conceptual level by requiring the definition of a security scheme that should provide for privacy protection (along with "integrity and confidentiality between the actors to ensure fair and secure data flow within the IFM [interoperable fare management] system (IFMS)" [3]). The security-related

[1] http://www.vdv.de/wir_ueber_uns/vdv_projekte/vdv_kernapplikation_efm.html

measures are defined in the respective security policy. Security management is performed by the Security Manager entity who is responsible for the implementation of the security policy by all actors concerned.

The standard prescribes that the privacy of a customer must be protected "as required by applicable laws" specifying the following rules:

- Only relevant personal data needed for the operation of the IFMS shall be requested from the Customer [the classic data minimization principle];
- The itemised disclosure of service consumption on an invoice shall be an option that can be chosen by the Customer;
- An IFM Actor may not disclose Customer-related information to third parties without specific authorisation from the Customer [user consent].
- Within the IFMS, the Customer-specific data shall be handled only in connection with the identification number of the Contract (implicit or explicit) between the Customer and Product Owner. A link between the Contract number and the name of the Customer may only be achieved by the contractual partner at the request of the Customer.

As it can be seen, the ISO EN 24014-1 standard rather coarsely specifies the privacy-related requirements which partially cover information linkage and illegal customer profiling (privacy threats 2 and 3, see section 3.). The standard, however, does not consider the more detailed recommendations concerning the further implementation of these requirements.

6.2 Data Interfaces Layer

EN 15320 The standard defines the logical structure of the data residing in the card, specifies an abstract interface for interaction between the card and the terminal (consists of two logical interfaces: the Card Data Interface and the Data Group Interface) and considers security through specification of the Security Subsystem (SSS). The latter is divided into Card Security Management System and Data Group Security Management System in order to correspond to the two logical interfaces. Security-related operations are defined in profiles (Card Profiles and Data Group Profiles respectively), see Figure 3.

The privacy-related issues are considered only indirectly in EN 15320 through the description of data groups containing privacy-relevant information (e.g. the *card holder* data group). If such data group is present, the necessary access control mechanisms together with encryption should be implemented in order to protect the customer's privacy (i.e. be included into the respective profiles of the SSS).

The division into two logical interfaces (Card Data Interface and Data Group Interface) provides for flexible implementation of access control schemes[1]. Specific security-related operations can be defined in the respective profiles and called whenever it is necessary to ensure proper execution of application commands. This mechanism may be used for processing of personal data in a privacy-respecting way therefore providing protection against unintended customer identification (namely,

[1]For example, in order to quickly and efficiently perform a ticket validation procedure, only the Card Data Interface is used, which speeds up the processes and saves resources.

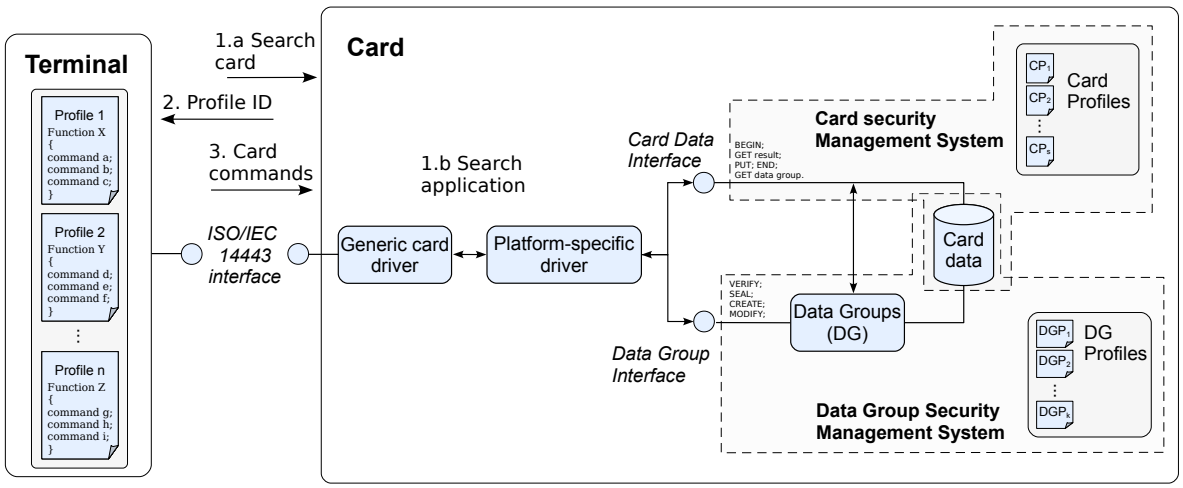

Figure 3: Interaction between a terminal and a card. Based on the processes description specified in EN 15320.

personal ID exposure and object's ID exposure, see section 3, threats 1(a)i and 1(a)ii respectively). The standard, however, does not explicitly address customer privacy and focuses solely on security issues.

EN 1545 Part 1 The structure of data elements residing in the card is considered, which is expressed according to ASN.1 (Abstract Syntax Notation 1). Privacy-relevant information is contained in several data elements presented in Table 2. These data can be protected by applying encryption and access control schemes defined at a logical level in the respective profiles of the security subsystem (SSS, see EN 15320 above) therefore covering the issues of personal ID exposure and object's ID exposure (privacy threats 1(a)i and 1(a)ii respectively, see section 3).

Table 2: Privacy-relevant fields in EN 1545-1.

Privacy-relevant field	**Description**
birth date	-
birth name	-
birth place	-
customer number	*customer reference number*
device ID	*can be linked to a particular customer*
e-mail address	-
telephone number	-
postal address	-
location ID	-
customer profile ID	*e.g. student, military, resident, etc.*
user data	*additional information about a customer*

Part 2 Data structures residing in the card are further specified according to the requirements of an interoperable fare management transport system (i.e. the requirements specified at higher layers of the standards stack, see Figure 1). This part of the standard focuses solely on the functional issues of a transport

system and does not consider privacy and security.

ISO/IEC 7816-4 The standard considers the issues of commands exchange as well as the retrieval of data structures and data objects residing in the card. Security and privacy are taken into account by specification of methods for secure messaging and a security architecture which defines access rights to files and data in the card. Access methods to the algorithms processed by the cards are considered as well [16].

6.3 Communication Interface Layer

ISO 14443 Parts 1-3 are required for connection establishment between the card and the terminal. The part 4 is optional and usually used for the cards with relatively high processing power. The standard does not consider any security- or privacy-related issues and focuses solely on functionality. Therefore, the issues of unintended customer identification during the anti-collision session and physical layer identification[1], which could be covered within the communication interface Layer, remain unconsidered.

6.4 A Short Summary

Summarizing, the standards composing the generic e-ticketing system primarily consider security for protection of transport companies' assets and maintaining the proper and reliable system functionality. The issues of customer privacy are seen more as a by-product of security without the additional measures specifically targeted at ensuring the privacy-respecting behaviour of the system. Table 3 summarizes the security and privacy measures considered in each standard.

Table 3: Security and privacy in the e-ticketing standards stack.

Standard	**Security**	**Privacy**
ISO EN 24014-1	- definition of security policy; - security management (by the Security Manager entity).	coarsely specified privacy requirements, targeted at compliance with the regulation
EN 15320	- Security Subsystem (SSS); - security-related operations are defined in profiles.	- privacy-relevant data groups; - protection through access control (AC) and encryption.
EN 1545	security-relevant fields	privacy-relevant fields, see Table 2
ISO/IEC 7816-4	- secure messaging; - security architecture with AC	security mechanisms can be applied to privacy-critical data
ISO 14443 (1-3)	not considered	not considered

Legend: – Architecture Layer
– Data interfaces Layer
– Communication interface Layer

[1]See privacy threats 1b and 1c in section 3.

7 E-ticketing: A Review of Proprietary Solutions with Respect to Privacy

In Europe, there exist several implementations of the e-ticketing paradigm, mainly on the national level (limited to a single country). The information concerning system specification and especially the security and privacy mechanisms is for the most part publicly unavailable, which is a hurdle when a review of privacy solutions in the area is considered. However, certain pieces of information are openly accessible.

7.1 ITSO

In the UK, ITSO (Integrated Transport Smartcard Organisation) has developed a specification for interoperable smart ticketing [17], which is similar to the guidelines of the respective standards (see the previous section). For example, according to the ITSO specification, security management is also performed through a Security Subsystem (SSS). Customer privacy is explicitly considered by the randomized encryption of the application ID[1] at the terminal side on each new session with the card (encryption unique to the current session). Therefore, only authorized entities (e.g. the application owner) can trace the complete history of card usage. This mechanism is aimed at protection against the unintended customer identification through the object's ID exposure (privacy threat 1(a)ii, see section 3).

In the publicly available version of ITSO specification, no mechanisms were found which explicitly specify the privacy-preserving processing of customer data (which would provide the protection against information linkage and illegal customer profiling, i.e. privacy threats 2 and 3, section 3.)

7.2 CALYPSO

Another popular proprietary e-ticketing standard developed in Europe is called "Calypso"[2]. According to [18], a Calypso application installed on the card possesses three types of 16-byte DESX or Triple-DES keys in order to modify different types of data: personal data, reload data, and validation data respectively. Whereas the messages are authenticated (MAC) within the secure session, the confidentiality is not considered, i.e. no message encryption is performed during data exchange between the card and the terminal [19] (e.g. during a validation procedure). Moreover, the *application serial number* is queried from the card *before* the secure session begins (it is used for key derivation in the terminal). Therefore, the transactions between the card and the terminal can be eavesdropped which leads to unintended customer identification and subsequent illegal profiling.

The *Holder Identity* field residing in the card can be protected by a PIN code [20], which must be presented during the access procedure (protection against personal ID exposure). Requiring a PIN code is, however, only an *optional* feature of the Calypso system [19].

In general, the Calypso system considers only the front-end security and privacy issues and leaves the implementation of back-end related mechanisms to public transport companies utilizing the Calypso technology for business [20].

[1] In the ITSO specification, it is called ITSO Shell Reference Number (ISRN) and is unique for each card. Therefore, it can be used for customer profiling if not protected properly.

[2] http://www.calypsonet-asso.org/index.php?rubrique=main_10.

There are known privacy issues connected with the e-ticketing Calypo-based systems. For example, the Belgian MOBIB[1] card enables remote read of the private information stored at the card (identity, birth date, zipcode as well as the tracks of the last three travels of the customer) by *any* compatible reader in the vicinity[2].

Summarizing, the customer privacy is weakly considered in the Calypso standard. Further effort is required to make it privacy-respecting.

7.3 Other Solutions

The e-ticketing systems based on MIFARE cards, such as Dutch OV-chipkaart, London's Oyster card, etc, can protect the privacy of their customers by utilizing the card's ability to generate random ID during the anti-collision session (therefore covering the respecting privacy threat 1b).

To this moment, this is the only publicly available information with respect to customer privacy in proprietary e-ticketing solutions that could be found.

8 Conclusion

This essay presented the preliminary results of state-of-the-art review with regard to privacy assessment of e-ticketing systems, which was carried out as part of the on-going work for my PhD dissertation. The analysis has shown that despite the plethora of tailor-made existing solutions, the one holistically treating the customer privacy in a cross-layered approach and across system components of an RFID-based e-ticketing system (back-end as well as front-end) is still missing. Therefore, more effort is required to develop a holistic framework which considers the creation of privacy-respecting e-ticketing systems.

References

[1] Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. User Privacy in Transport Systems Based on RFID E-Tickets. In *Workshop on Privacy in Location-Based Applications (PILBA 2008)*, volume 5283 of *Lecture Notes in Computer Sciences*. Springer-Verlag, October 2008. Malaga, Spain.

[2] Smart cards move onwards. *Card Technology Today*, 15(10):12 – 15, 2003.

[3] Public transport – Interoperable fare management system – Part 1: Architecture (ISO 24014-1:2007). http://www.iso.org/iso/catalogue_detail?csnumber=41985, 2007.

[4] Gilles de Chantérac and Jean-Louis Graindorge. Focus Paper on Privacy in Transport IFM Applications. IFM Project, http://www.ifm-project.eu/fileadmin/WP2/Draft_Deliverable_2.2.pdf, March 2009. Draft Deliverable 2.2.

[5] Cord Bartels, Harald Kelter, Rainer Oberweis, and Birger Rosenberg. TR 03126 - Technische Richtlinie für den sicheren RFID-Einsatz. TR 03126-1: Einsatzgebiet

[1] http://www.stib.be/mobib.html?l=en

[2] http://blog.security4all.be/2009/01/privacy-failure-in-belgian-rfid.html, http://sites.uclouvain.be/security/mobib.html

"eTicketing im öffentlichen Personenverkehr", 2009. Bundesamt für Sicherheit in der Informationstechnik, Deutschland.

[6] Davide Zanetti, Pascal Sachs, and Srdjan Capkun. On the Practicality of UHF RFID Fingerprinting: How Real is the RFID Tracking Problem? In Simone Fischer-Hbner and Nicholas Hopper, editors, *Privacy Enhancing Technologies*, volume 6794 of *Lecture Notes in Computer Science*, pages 97–116. Springer Berlin / Heidelberg, 2011.

[7] Martin Rost and Andreas Pfitzmann. Datenschutz-schutzziele — revisited. *Datenschutz und Datensicherheit - DuD*, 33:353–358, 2009.

[8] Harald Zwingelberg and Marit Hansen. Privacy Protection Goals and Their Application to eID Systems. In *IFIP Summer School 2011*, 2011.

[9] Ari Juels and Ravikanth Pappu. Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In *Financial Cryptography '03*, pages 103–121. Springer-Verlag, 2002.

[10] Tong-Lee Lim, Tieyan Li, and Sze-Ling Yeo. Randomized Bit Encoding for Stronger Backward Channel Protection in RFID Systems. In *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, PERCOM '08, pages 40–49, Washington, DC, USA, 2008. IEEE Computer Society.

[11] Wonjoon Choi and Byeong-hee Roh. Backward Channel Protection Method for RFID Security Schemes Based on Tree-Walking Algorithms. In Marina Gavrilova, Osvaldo Gervasi, Vipin Kumar, C. Tan, David Taniar, Antonio Laganá, Youngsong Mun, and Hyunseung Choo, editors, *Computational Science and Its Applications - ICCSA 2006*, volume 3983 of *Lecture Notes in Computer Science*, pages 279–287. Springer Berlin / Heidelberg, 2006.

[12] Tong-Lee Lim, Tieyan Li, and Sze-Ling Yeo. A Cross-layer Framework for Privacy Enhancement in RFID systems. *Pervasive and Mobile Computing*, 4(6):889 – 905, 2008.

[13] Ivan Gudymenko. Protection of the Users' Privacy in Ubiquitous RFID Systems. Master's thesis, Technische Universität Dresden, Faculty of Computer Science, December 2011.

[14] ISO 14443 Standards family. Identification cards – Contactless integrated circuit cards – Proximity cards. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39693.

[15] Silvester Prakasam and Adeline Wang. Implementing Vehicle Location System for Public Buses in Singapore. *Journal of Institute of Engineers*, 44.

[16] ISO/IEC 7816-4:2005. Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36134, 2005.

[17] ITSO Technical Specification 1000: Interoperable public transport ticketing using contactless smart customer media. Version V2.1.4. http://www.itso.org.uk/page49/Home/Itso-Specification, 2010.

[18] Frederic Levy. Calypso Functional Presentation. SAM and Key Management. http://www.calypsostandard.net/index.php?option=com_docman&task=doc_download&gid=9&Itemid=40, 2010.

[19] Innovatron-RATP-SNCF. Calypso functional specification. Card application. http://www.calypsostandard.net/index.php?option=com_docman&task=doc_download&gid=3&Itemid=40, 2010.

[20] Calypso Networks Association. Calypso Handbook. http://www.calypsonet-asso.org/downloads/100324-CalypsoHandbook-11.pdf, 2010.