TECHNISCHE UNIVERSITÄT DRESDEN

Europäische Union

Europa fördert Sachsen. ESF Europäischer Sozialfonds

Fakultät Informatik Institut für Systemarchitektur

Privacy-preserving E-ticketing Systems for Public Transport Based on RFID/NFC Technologies

Dissertation Summary

Submitted to the Faculty of Computer Science, TU Dresden,
in Partial Fulfillment of the Requirements for the Degree of Dr.-Ing.

Presented by M.C.S. **Ivan Gudymenko**

Born on 15 December 1986 in Mykolaiv, Ukraine

Scientific Advisers:

Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill	TU Dresden, Germany
Prof. Dr. habil. Simone Fischer-Hübner	Karlstad University, Sweden
Dr.-Ing. Katrin-Borcea Pfitzmann	TU Dresden, Germany

Dresden, December 18, 2014

1 Introduction

Pervasive digitization of human environment has dramatically changed our everyday lives. New technologies which have become an integral part of our daily routine have deeply affected our perception of the surrounding world and have opened qualitatively new opportunities. In an urban environment, the influence of such changes is especially tangible and acute. For example, ubiquitous computing (also commonly referred to as UbiComp) is a pure vision no more and has transformed the digital world dramatically. Pervasive use of smartphones, integration of processing power into various artefacts as well as the overall miniaturization of computing devices can already be witnessed on a daily basis even by laypersons. In particular, transport being an integral part of any urban ecosystem has been affected by these changes. Consequently, public transport systems have undergone transformation as well and are currently dynamically evolving. In many cities around the world, the concept of the so-called electronic ticketing (e-ticketing) is being extensively used for issuing travel permissions which may eventually result in conventional paper-based tickets being completely phased out already in the nearest future. Opal Card in Sydney [1], Oyster Card in London [2], Touch & Travel in Germany [3] and many more are all the examples of how well the e-ticketing concept has been accepted both by customers and public transport companies.

Despite numerous benefits provided by such e-ticketing systems for public transport, serious privacy concern arise. The main reason lies in the fact that using these systems may imply the dramatic multiplication of digital traces left by individuals, also beyond the transport scope. Unfortunately, there has been little effort so far to explicitly tackle this issue. There is still not enough motivation and public pressure imposed on industry to invest into privacy. In academia, the majority of solutions targeted at this problem quite often limit the real-world pertinence of the resultant privacy-preserving concepts due to the fact that inherent advantages of e-ticketing systems for public transport cannot be fully leveraged.

This thesis is aimed at solving the aforementioned problem by providing a privacy-preserving framework which can be used for developing e-ticketing systems for public transport with privacy protection integrated from the outset. At the same time, the advantages of e-ticketing such as fine-grained billing, flexible pricing schemes, and transparent use (which are often the main drivers for public to roll out such systems) can be retained.

2 Core Technologies Enabling the Realization of E-ticketing

The classic and by far the most widespread technology for realization of e-ticketing systems in the front-end is radio frequency identification (RFID). Another promising technology very closely related to RFID is the so-called near field communication (NFC) currently gaining rapid momentum and being actively integrated into many smartphones appearing on the market. Therefore, in this dissertation, the focus is made on RFID- and NFC-based e-ticketing systems. Since the area of NFC and especially RFID is rather broad being used in different domains and incorporating several standards, the ones specific to the e-ticketing domain were focused on.

3 Main Goals and Research Questions

The basic architecture of an e-ticketing system for public transport essentially consists of e-tickets residing on a user device (a smart card or an NFC-enabled smartphone), terminals validating e-tickets, and the back-end which controls the system. **The main goal** of this dissertation is to develop a framework for building a loosely-coupled privacy-preserving e-ticketing system which *(1)* allows for local validation of e-tickets and *(2)* supports fine-grained billing for registered customers. Based on this, specific research questions (RQ) have been derived for this work which are summarized below.

Research Questions

RQ 1. How to provide for a privacy-preserving local validation at the terminal side such that:

a) valid e-tickets remain anonymous to the terminal;

b) invalid e-tickets are rejected.

RQ 2. How to allow for privacy-preserving travel records processing in the back-end such that:

a) fine-grained billing for the registered tickets is possible;

b) direct identification of customers is prevented.

4 Thesis Contributions

The contribution of this thesis is a privacy-preserving framework which explicitly addresses the issues of privacy protection in e-ticketing systems for public transport (ESPT). On the one hand, it allows for the implementation of flexible pricing schemes and fine-grained billing. A transport authority, therefore, would be able to fully leverage the whole potential of such systems. On the other hand, our solution addresses privacy protection from the outset through the specific system design. Moreover, in contrast to several other solutions, the developed framework is based on a loosely-coupled architecture implying that terminals do not have to maintain permanent real-time connection to the back-end in order to serve check-in/check-out requests in the front-end. The main contributions of the thesis are summarized below.

1. Design and evaluation of a framework allowing to develop privacy-preserving e-ticketing systems for public transport.
   a) The developed approach enables for the implementation of fine-grained billing and transparent tariff schemes in a natural way.
   b) At the same time, privacy properties can be retained.
2. Important findings with respect to practical realization of interactive privacy-preserving protocols on end user devices (RFID smart cards and NFC-enabled smart phones):
   a) The issues concerning the implementation of interactive protocols via an NFC interface in Android-based smart phones have been discussed.
   b) The hurdles encountered while applying the protocols requiring the non-standard cryptographic primitives to conventional smart cards were described.
3. Classification of the field with respect to privacy preservation in the context of public transport systems based on e-ticketing was presented.

The core findings of the thesis were published in the following conferences:

- Ivan Gudymenko. A Privacy-Preserving E-Ticketing System for Public Transportation Supporting Fine-Granular Billing and Local Validation. In *Proceedings of the 7th International Conference on Security of Information and Networks, Glasgow, UK*, SIN '14, New York, NY, USA, 2014. ACM. Best paper award in section "Assuarance and Trust"
- Ivan Gudymenko, Felipe Sousa, and Stefan Köpsell. A Simple and Secure E-Ticketing System for Intelligent Public Transportation based on NFC. In *The First International Conference on IoT in Urban Space, Rome, Italy*, Urb-IoT, New York, NY, USA, 2014. ACM

- Ivan Gudymenko. On Protection of the User's Privacy in Ubiquitous E-ticketing Systems Based on RFID and NFC Technologies. In *PECCS 2013 - Proceedings of the 3rd International Conference on Pervasive Embedded Computing and Communication Systems*. SciTePress, February 2013
- Florian Kerschbaum, Hoon Wei Lim, and Ivan Gudymenko. Privacy-Preserving Billing for e-Ticketing Systems in Public Transportation. In *Proceedings of the 12th ACM workshop on privacy in the electronic society, WPES'2013* , WPES '13, pages 143–154, New York, NY, USA, July 2013. ACM, (as a co-author)

5 Related Work

In order to provide for an adequate related work analysis, a set of core requirements posed to a privacy-preserving e-ticketing system was elaborated on in the thesis. The respective summary is depicted in Table 1. Moreover, an attacker model was created as well which is presented in Table 2.

Table 1: A summary of core requirements

1. *Privacy*
   a) *Privacy against external observers.* An external attacker must be prevented from deriving any Personally Identifiable Information (PII) from interaction between e-tickets and terminals in the front-end.
   b) *Privacy against terminals.* Terminals must be prohibited from tracking and distinguishing between valid e-tickets as well as from identifying the users associated with them.
   c) *Privacy against the back-end.* The back-end is allowed to correlate travel records related to a single e-ticket while being prohibited from identifying the users associated with e-tickets.
2. *Fine-grained billing support*
3. *Loose-coupling*
4. *Efficiency.* Check-in/out events handling must comply with the timing requirements.
5. *Multilateral security*

First approaches considering the problem of privacy protection in e-ticketing systems for public transport originated from the area of privacy-preserving RFID systems. With this respect, the solution due to Okubo *et al.* [8] commonly referred to as OSK is particularly suited for lightweight RFID authentication. Despite providing for untraceability and unlinkability against an observing attacker and a terminal, the OSK protocol has fundamental limitations such as a limited number of authentication sessions, tightly-coupled back-end which must process all front-end requests in real time as well as the susceptibility to replay attacks. Moreover, OSK only provides a one-way authentication of an RFID device to the terminal. Similarly, the SVW framework due to Sadeghi *et al.* [9] has the same disadvantage. In contrast to OSK and SVW, the approach devised by Song and Mitchell [10] (SM) allows for *mutual* authentication. Similarly to the OSK protocol, SM provides RFID tag's anonymity and untraceability against terminals as well as it follows the assumption that the back-end is fully trusted. Unlike SVW, both OSK and SM require real-time connection to the back-end, since terminals essentially relay communication between RFID devices managing e-tickets and the back-end. The approach presented by Avoine *et al.* [11] (ALM) overcomes this issue by leveraging the concept of terminal-specific access lists used for mutual authentication. However, this solution similarly relies on the assumption that the back-end is fully trusted and moreover has linear complexity in the number of all devices to be authenticated. Garcia and Rossum (GR) presented an alternative solution in [12] which is based on regular updates of terminal secrets and does not require the calculation of

terminal-specific access lists in the back-end. However, no mutual authentication is provided by their approach. Moreover, is has linear complexity for RFID tag authentication as well as it considers only a limited number of authentication sessions between two consecutive terminal updates.

Another class of approaches in the area of privacy-preserving e-ticketing systems is based on e-cash and essentially inherits its decent privacy properties. With this respect, Heydt-Benjamin *et al.* [13] devised a privacy-preserving framework explicitly targeting e-ticketing systems for public transport. Similarly, the work of Baldimtsi *et al.* [14] presented a framework based on recent advances in e-cash which unlike the former approach does not rely on the back-end being always online to serve check-in/check-out requests in the front-end. Unfortunately, one of the main limitation of the solutions based on e-cash is that they inherently prohibit the deployment of fine-grained billing and flexible pricing schemes (which are among the core advantages of e-ticketing).

Summarizing, it can be concluded that none of the reviewed approaches fully satisfies the core requirements posed to privacy-preserving e-ticketing systems for public transport (see Table 3).

Table 2: The adopted attacker model

1. *(Outsider)* **External observers** can tap the wireless communication between terminals and e-tickets in the front-end.
   → No derivation of PII should be possible in this case.
2. *(Insider)* **Terminals** can perform additional analysis of communication data and logs maintained, may leak information (e.g., due to a buffer overflow attack mounted via the wireless interface).
   → No tracking of valid e-tickets, distinguishing between them or identification of user identities associated with e-tickets should be allowed.
3. *(Insider)* **Back-end** can process all information pieces under its control, relate them together and analyze.
   → No identification of users associated with e-tickets should be possible.

Table 3: Related work summary. Advantages are marked with ✓.

Criteria	**The most relevant approaches Reviewed**						
	PAYG [14]	HCDF [13]	SVW [9]	GR [12]	ALM [11]	OSK [8]	SM [10]
Tight coupling	no ✓	yes	no ✓	no ✓	no ✓	yes	yes
Anonymity against term.	yes ✓	yes ✓	no	no	no	yes ✓	yes ✓
Untraceab. against term.	yes ✓	yes ✓	no	no	no	yes ✓	yes ✓
Mutual authentication	no	no	no	no	yes ✓	no	yes ✓
Fine-grained billing possible	no	no	yes ✓	yes ✓	yes ✓	yes ✓	yes ✓
Terminals are trusted	no ✓	no ✓	yes	yes	yes	no ✓	no ✓
The back-end is trusted	no ✓	no ✓	yes	yes	yes	yes	yes

6 Suggested Solution

The developed solution represents a framework allowing for the development of privacy-preserving e-ticketing systems for public transport which fully satisfy the core requirements summarized in Table 1. Namely, during check-in/check-out events, terminals gain no further information about the valid e-tickets beyond the mere fact of their validity. Therefore, terminals can not trace e-tickets or correlate

different sessions to a single e-ticket. At the same time, the invalid e-tickets are rejected by checking against a terminal-side blacklist. Moreover, in the back-end, no user identification is possible due to the developed pseudonymisation scheme which essentially establishes a privacy overlay in the system on top of which fine-grained billing is nevertheless possible. Lastly, an observing entity exogenous (external) to the system gains no information on the e-ticket by observing the communication between terminals and e-tickets. Thus, our solution goes in line with adopted attacker model summarized in Table 2.

6.1 Main building blocks

Our solution is essentially comprised of three core building blocks:

1. *Mutual authentication* between an e-ticket and a terminal (system front-end). In this case, the front-end of e-ticketing system for public transport (ESPT) is in focus, since the backbone communication can be secured using fully-fledged, well-established standard mechanisms.

2. *Local revocation* of invalid e-tickets at the terminal side without the need to consult the back-end database in a timely fashion (system front-end), supports loose-coupling.

3. *Path reconstruction.* Correlating different travel rides to a user pseudonym for billing purposes (system back-end).

All of the three aforementioned building blocks (depicted in Figure 1) must be implemented in a privacy-preserving way corresponding to the adopted attacker model and being conform to the core requirements (see Table 1). In our solution, mutual authentication was implemented through a slightly modified certificate-based authentication. In order to provide for the second building block (local revocation), a custom blacklisting scheme was developed. Path reconstruction was realized through a custom pseudonymisation scheme.

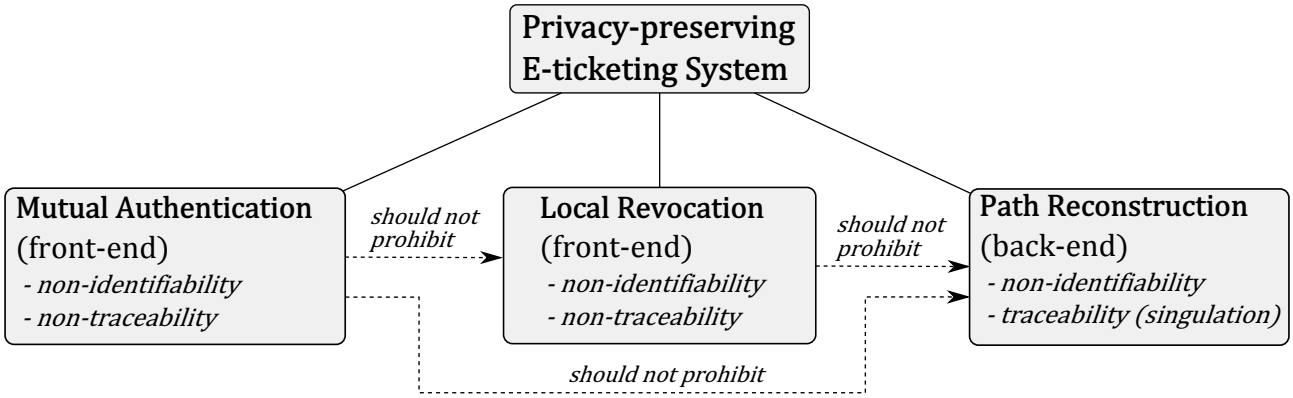

Figure 1: Main building blocks of our solution. Privacy properties such as non-identifiability and untraceability refer to an e-ticket (either against a terminal in the front-end or against the back-end system).

6.2 Solution Outline

Our privacy-preserving framework follows the principles of information minimization and task division between non-colluding entities. The solution essentially considers two distinct entities: *(1)* a transport authority (TA) and *(2)* an external trusted third party (TTP), see Figure 2. TA represents a public transport company which provides transport services. TTP acts as a trusted mediator between a transport authority (which maintains the public transport system) and its end users. The main idea

behind this concept is the following. In order to issue a bill, the back-end of a TA does not necessarily have to possess identifying information about a particular user of an e-ticket. It merely needs to be able to correlate different rides performed by a customer to a certain pseudonym which has been negotiated with a TTP in advance and based on this information to apply the deployed pricing schemes with the subsequent billing procedure. The resultant bill together with the corresponding pseudonym is periodically sent to the TTP. The latter has no knowledge of travel history of a customer but is solely aware of the overall bill and the user behind the pseudonym. Individual payments are then forwarded to the TA by the TTP in an aggregated form. In addition, the rides history could be stored at the user device (e.g. a smartphone) so that it can be locally viewed by a customer later. Thus, the TA trusts the TTP that users are correctly billed (together with payment enforcement) while customers rely on the TTP to protect their privacy and forward payments to the TA. In essence, the approach outlined above creates a privacy overlay with respect to the sensitive data pertaining to users. Thus, the back-end of a TA (alternatively, of several TAs for interoperability) is operating on this abstract layer without directly processing the identifiable information of customers. An important condition here is that the TTP does not collude with the TA to defeat privacy protection provided by the solution.

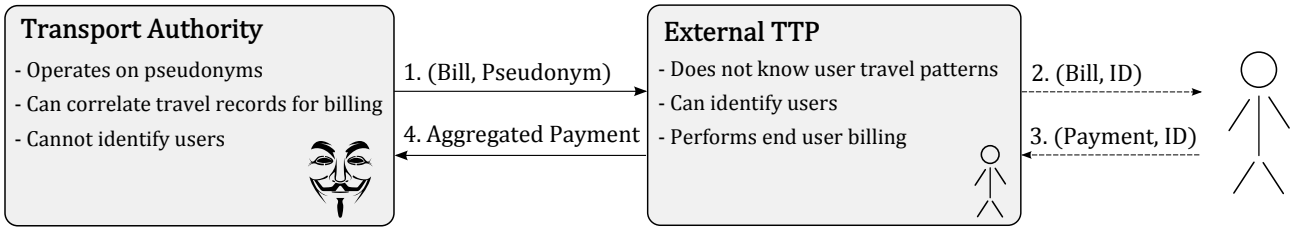

Figure 2: A privacy-preserving framework: an overview.

6.3 Framework Information Flow

6.3.1 Initialization

Before being able to actively use the transport system, each customer has to engage into an initialization phase with the TTP. This can be carried out in one of the following ways: *(1)* via a special issuing machine, *(2)* directly at the customer office of a transport authority, or *(3)* via the internet. On registering the customer, the TTP creates the respective pseudonym P_i^T and forwards it to the TA. The latter further transforms the received pseudonym into its encrypted form P_i^A and operates on it The customer in turn gets the necessary credentials from the TTP to start using the system, namely: a TA public key k_{ta}^+, a key pair corresponding to the subscription group (e.g. a monthly or yearly pass) (k_{gr}^+, k_{gr}^-), as well as the specifically created customer pseudonym P_i^T (together with its TA-form P_i^A). Note that a public key is denoted as k^+ and a private one as k^-. The received key pair is signed by the TA and can be viewed as a kind of a digital certificate.

6.3.2 System in Action

Front-end (time-critical). On entering the public transport system, a user performs check-in at the entrance terminal. This involves three stages: *(1)* a secure session establishment, *(2)* mutual authentication, and *(3)* blacklist check (see Figure 3). The aforementioned processes must be handled in a timely fashion, since a check-in/check-out operation implies a customer holding his/her device near the terminal waiting to begin/end or to continue the travel. The secure session can be established either using an algorithm defined by the e-ticketing application itself (e.g., through the application-defined Diffie-Hellman key agreement) or alternatively by leveraging the standard techniques defined in ISO 7816-4 [15] or in NFC-SEC-01 [16]. Note that depending on the way the secure session has

been established during the first stage, additional binding of the exchanged keying material (e.g., DH ephemeral keys) to the corresponding certificates may be required to prevent man-in-the-middle[1] attacks. The subsequent communication between an e-ticket and a terminal is, therefore, secured against an observing attacker. Afterwards, mutual authentication between an e-ticket and a terminal is performed as follows. The terminal has its unique public key k_T^+ signed by the back-end. The e-ticket uses its group key pair (k_{gr}^+, k_{gr}^-) which is signed by the TA back-end as well. Mutual authentication is then essentially performed according to the certificate-based challenge-response. Lastly, the terminal (locally) checks if the credentials of the current e-ticket have not been revoked by consulting the blacklist (see *BL Check* in Figure 3). This is performed in a privacy-preserving way (in contrast to the majority of conventional systems). That is, each e-ticket stays anonymous and untraceable against the terminal as long as it has not been included into a terminal-side black list. The details on privacy-preserving blacklist check can be found in the full version of the dissertation. On successful check, the terminal creates the so-called travel record corresponding to the current check-in/check-out event. It usually contains a timestamp, location, and other pieces of information pertaining to the e-ticket.

Back-end (non-real time). A set of travel records maintained by each terminal is regularly sent to the back-end system via the backbone network where they are processed for billing purposes (Figure 3, *Billing*). Terminal-side blacklists are regularly updated as well. The frequency of such updates is mainly determined by the connection type between terminals and the back-end (e.g., nightly updates as considered in [11] or more frequent updates if the connection allows). In the back-end, different travel records are sorted with respect to the e-ticket they pertain to. Hereinafter, this is referred to as singulation (see Figure 3). After the singulation phase, the respective billing policies are applied resulting in the overall bill for a certain customer pseudonym. A detailed description of the developed pseudonymisation scheme can be found in the full version of the thesis.

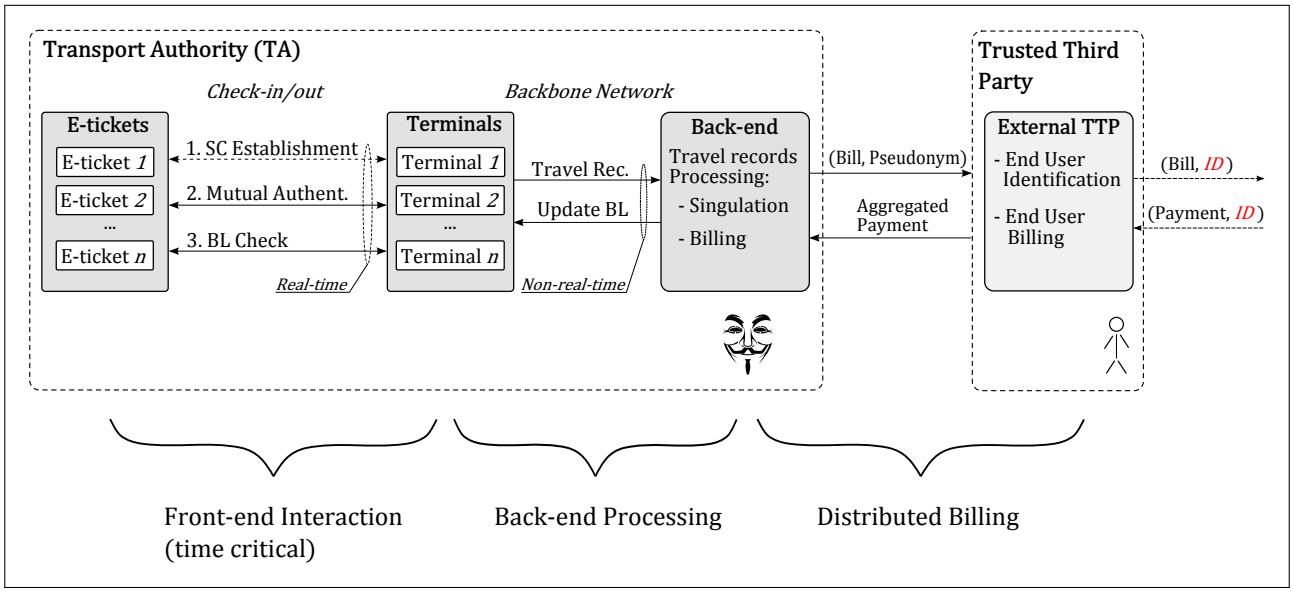

Figure 3: The developed privacy-preserving framework. *BL* stands for blacklist, *SC* – for secure channel.

[1]It has to be mentioned, however, that due to the physical properties of communication between terminals and e-tickets, man-in-the-middle attacks (in contrast to relay attacks) mounted on such wireless interface are extremely unlikely in practice [17].

7 Evaluation Results

The developed privacy-preserving framework fully satisfies the core requirements presented in Table 1. The respective analysis can be found in the full version of the dissertation. In order to assess the framework from a practical side, the most critical part of it considering the front-end interaction has been validated using the two prototypes developed for the NFC and RFID platforms. In the first case, a user device was represented by an NFC-enabled smartphone, namely a middle class Samsung Galaxy Nexus GT-I9250. In the second case, an RFID-enabled smart card acted as a user device. More specifically, an NXP J3A080 Java smart card was used. Framework performance was assessed based on the overall runtime of a single front-end session between a user device and a terminal with respect to the number of elements in the blacklist maintained by the terminal (blacklist check is the most costly operation). The evaluation results for RFID and NFC prototypes are depicted in Figure 4 and Figure 5 respectively. During the analysis, two performance areas can be determined which correspond to the respective runtimes and blacklist sizes, namely *(1)* acceptable performance (AP) area and *(2)* optimal performance (OP) area. The former corresponds to runtimes below 2000 *ms* whereas the latter is bounded by runtimes below 1000 *ms*. These particular figures have been determined during the analysis of real-world systems. The core trade-off between the runtime and the blacklist size can be clearly observed in the graphs. AP and OP boundaries outline the areas which can be considered in a real setting. As it can be seen, the performance of the NFC prototype is better compared to the RFID one. Due to inherent resource constraints of the smart card platform, the performance of the RFID prototype is less efficient with no OP area observed. However, for both cases the real-world pertinence of the developed framework could be demonstrated. The detailed evaluation can be found in the full version of the dissertation.

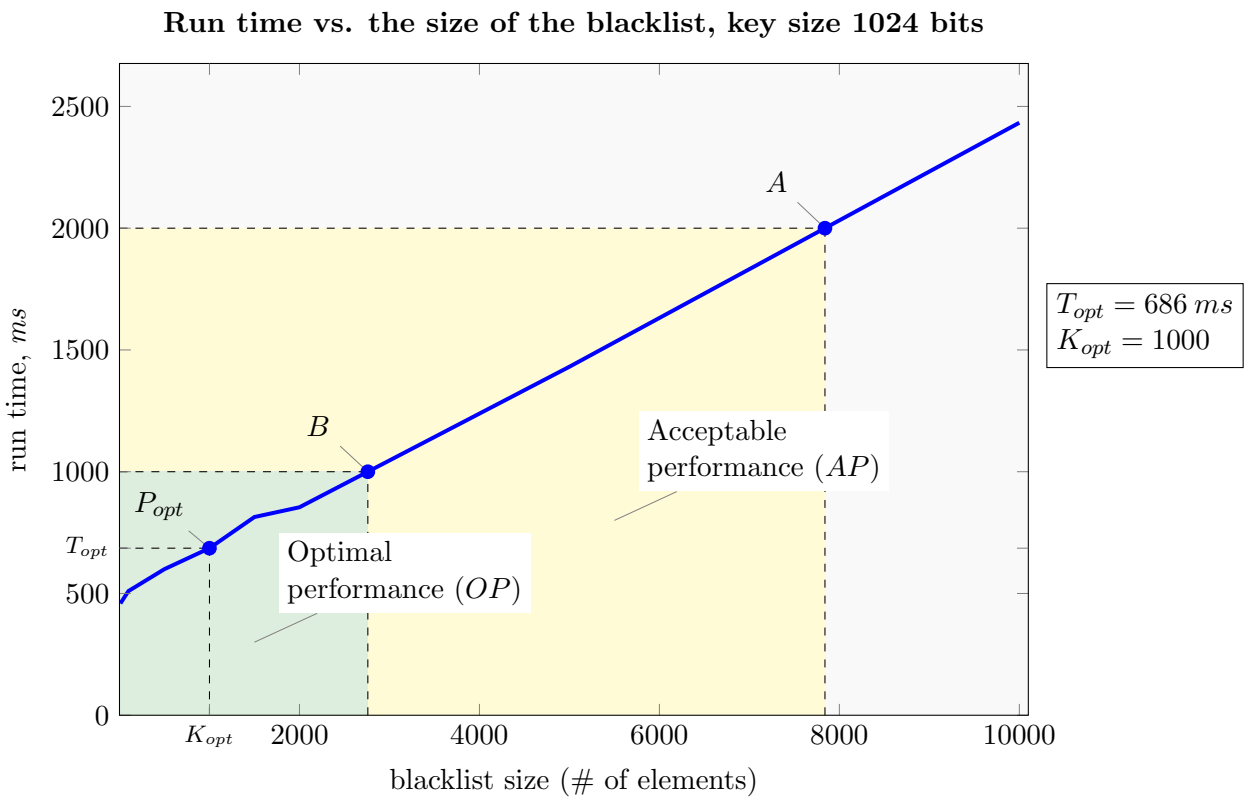

Figure 4: NFC prototype. Performance of check-in/out events handling with respect to the size of the blacklist. Key sizes used are 1024 bits.

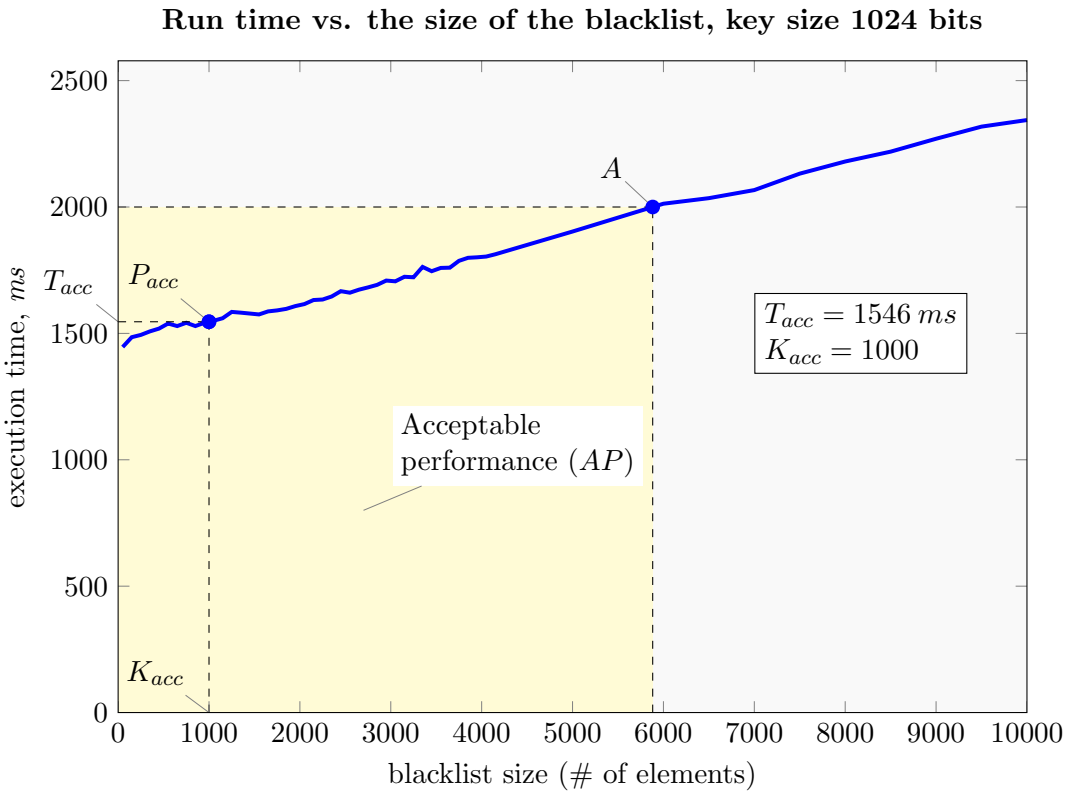

Figure 5: RFID prototype. Performance of check-in/out events handling with respect to the size of the blacklist. Key sizes used are 1024 bits.

8 Covering Research Questions

All research questions discussed in Section 3 could be fully answered within the thesis. Each research question is separately discussed below.

Research Question 1.

How to provide for a privacy-preserving local validation at the terminal side such that:

a) valid e-tickets remain anonymous to the terminal;

b) invalid e-tickets are rejected.

As discussed above, the developed solution essentially consists of three main building blocks: *(1)* mutual authentication, *(2)* local revocation, and *(3)* path reconstruction. The suggested mutual authentication mechanism ensures that *(a)* user devices (managing corresponding e-tickets) engage into full communication sessions only with authorized terminals, *(b)* terminals can check the validity of travel permission and at the same time learn no further information on the e-ticket itself (no tracking or identifying the associated user is possible). Furthermore, the developed approach for local revocation ensures that the blacklisted e-tickets (for example, the ones associated with the customers who failed to pay their bills, or in case of theft, etc.) are rejected without negatively affecting the privacy of those users associated with the valid e-tickets. Therefore, the *research question 1* could be fully answered.

Research Question 2.

How to allow for privacy-preserving travel records processing in the back-end such that:

a) fine-grained billing for the registered tickets is possible;

b) direct identification of customers is prevented.

The third building block of the suggested solution – path reconstruction – realized in the form of a custom pseudonymisation scheme ensures that on the one hand, the back-end has enough information to perform fine-grained billing (possibly taking into account different pricing schemes and discounts) and on the other hand is prohibited from identifying customers associated with e-tickets. The developed pseudonymisation scheme essentially creates a privacy overlay enabling travel records processing in the back-end with the desired privacy properties. Consequently, an answer to the second research question is thereby provided.

Summarizing, it can be concluded that both research questions could be answered within the thesis.

Bibliography

[1] Transport for NSW. Opal Card. http://www.transport.nsw.gov.au/content/opal-card, 2014. Accessed on 10.06.2014.

[2] Transport for London. Oyster Online. https://oyster.tfl.gov.uk/oyster/entry.do, 2012. Accessed on 30.10.2012.

[3] Transport for NSW. Touch & Travel. http://www.touchandtravel.de/, 2014. Accessed on 10.06.2014.

[4] Ivan Gudymenko. A Privacy-Preserving E-Ticketing System for Public Transportation Supporting Fine-Granular Billing and Local Validation. In *Proceedings of the 7th International Conference on Security of Information and Networks, Glasgow, UK*, SIN '14, New York, NY, USA, 2014. ACM. Best paper award in section "Assuarance and Trust".

[5] Ivan Gudymenko, Felipe Sousa, and Stefan Köpsell. A Simple and Secure E-Ticketing System for Intelligent Public Transportation based on NFC. In *The First International Conference on IoT in Urban Space, Rome, Italy*, Urb-IoT, New York, NY, USA, 2014. ACM.

[6] Ivan Gudymenko. On Protection of the User's Privacy in Ubiquitous E-ticketing Systems Based on RFID and NFC Technologies. In *PECCS 2013 - Proceedings of the 3rd International Conference on Pervasive Embedded Computing and Communication Systems*. SciTePress, February 2013.

[7] Florian Kerschbaum, Hoon Wei Lim, and Ivan Gudymenko. Privacy-Preserving Billing for e-Ticketing Systems in Public Transportation. In *Proceedings of the 12th ACM workshop on privacy in the electronic society, WPES'2013* , WPES '13, pages 143–154, New York, NY, USA, July 2013. ACM.

[8] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Cryptographic Approach to "Privacy-Friendly" Tags. In *In RFID Privacy Workshop*, 2003.

[9] 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.

[10] Boyeon Song and Chris J. Mitchell. Scalable RFID security protocols supporting tag ownership transfer. *Comput. Commun.*, 34(4):556–566, apr 2011.

[11] Gildas Avoine, Cédric Lauradoux, and Tania Martin. When Compromised Readers Meet RFID. In Heung Youl Youm and Moti Yung, editors, *Information Security Applications*, volume 5932 of *Lecture Notes in Computer Science*, pages 36–50. Springer Berlin Heidelberg, 2009.

[12] Flavio D. Garcia and Peter Rossum. Modeling Privacy for Off-Line RFID Systems. In Dieter Gollmann, Jean-Louis Lanet, and Julien Iguchi-Cartigny, editors, *Smart Card Research and Advanced Application*, volume 6035 of *Lecture Notes in Computer Science*, pages 194–208. Springer Berlin Heidelberg, 2010.

[13] Thomas S. Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu. Privacy for Public Transportation. In *Proceedings of the 6th international conference on Privacy Enhancing Technologies*, PET'06, pages 1–19, Berlin, Heidelberg, 2006. Springer-Verlag.

[14] Foteini Baldimtsi, Gesine Hinterwalder, Andy Rupp, Anna Lysyanskaya, Christof Paar, and Wayne P. Burleson. Pay as you go. In *Workshop on hot topics in privacy enhancing technologies, HotPETSs 2012*. http://petsymposium.org/2012/papers/hotpets12-8-pay.pdf, 2012.

[15] ISO. 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.

[16] ECMA International. NFC-SEC. NFCIP-1 Security Services and Protocol. Cryptography Standard using ECDH and AES, 2008. White paper.

[17] E. Haselsteiner and K. Breitfuß. Security in Near Field Communication (NFC). Strengths and Weeknesses. In *Workshop on RFID Security 2006 (RFIDSec'06)*, Graz, Austria, 2006.