A Privacy-Preserving Contactless Transport Service for NFC Smartphones

Ghada Arfaoui, Sébastien Gambs, Patrick Lacharme, Jean-François Lalande, Lescuyer Roch, Jean-Claude Paillès

A Privacy-Preserving Contactless Transport Service for NFC Smartphones

Ghada Arfaoui[14], Sébastien Gambs[2], Patrick Lacharme[3], Jean-Francois Lalande[42], Roch Lescuyer[5*], and Jean-Claude Paillès[3]

[1] Orange Labs, Caen, France
ghada.arfaoui@orange.com,
[2] SUPELEC/Inria/CNRS/Université de Rennes 1, IRISA (UMR 6074)
sebastien.gambs@irisa.fr
[3] Laboratoire GREYC (Unicaen, Ensicaen, CNRS), UMR 6072, F-14032 Caen
patrick.lacharme@ensicaen.fr
jean-claude.pailles@unicaen.fr
[4] ENSI de Bourges, Univ. Orléans, LIFO, EA 4022, F-18020, Bourges, France
jean-francois.lalande@ensi-bourges.fr
[5] Morpho, F-92130, Issy-Les-Moulineaux, France
roch.lescuyer@morpho.com

Abstract. The development of NFC-enabled smartphones has paved the way to new applications such as mobile payment (m-payment) and mobile ticketing (m-ticketing). However, often the privacy of users of such services is either not taken into account or based on simple pseudonyms, which does not offer strong privacy properties such as the unlinkability of transactions and minimal information leakage. In this paper, we introduce a lightweight privacy-preserving contactless transport service that uses the SIM card as a secure element. Our implementation of this service uses a group signature protocol in which costly cryptographic operations are delegated to the mobile phone.

1 Introduction

The design of a secure and private mobile transport service is one of the most challenging application for NFC-enabled device. In particular, this service requires a proof of the customer's identity and of the validity of his attributes in relation with the product. In transport systems, these attributes are controlled by the service provider and stored on the user's smartphone. Thus, the user's personal data are exposed to any type of surveillance from the service provider.

In this paper, we introduce an architecture in which the user's identity can be dematerialized in a secure element, in our case, the SIM card. More precisely, we propose a privacy-preserving identity management system for transport service, whose security is based on the combination of a secure element embedded in the smartphone together with the use of a privacy enhancing cryptographic protocol.

[*] This work was done while the fifth author was at Ensicaen, Caen, France.

2 M-ticketing Solutions for Transportation

CALYPSO is a standard describing contactless transactions between a smart card and a reader that is used in transport applications [1]. This standard has been developed by a European consortium composed of transportation operators such as the Belgium STIB and the French RATP. For instance in France, the Navigo pass is based on the Calypso standard. This standard specifies all details of transactions related to e-ticketing for transport service ranging from the purchase of the tickets to their uses. Unfortunately, this standard does not propose any technical solution for protecting the privacy of users.

The German FRDB has proposed the service Touch and Travel (T&T), a mobile ticketing service [2] since 2008. The user must first subscribe to the service by showing his identity along with his bank account. Afterwards, he gets a user number and a PIN allowing him to use the T&T application. To travel from a station A to a station B, a user must start the T&T application upon departure by using either a touchpoint if available in the station or a GPS location or a location based on network cell. Arriving to the station B, the user must indicate the end of his trip. When controlled, the T&T application generates and displays a QR code to prove that the payment for the trip is proceeding normally. However, a recent study [2] has shown that T&T does not respect the privacy requirements as the application T&T stores the list of all recent trips in a centralized database.

Recently, it has been proposed an identity verification ticketing scheme that is embedded in a trusted execution environment [3]. This solution complies with a major functional requirement: carrying out an identity verification transaction should require less than 300 milliseconds (ms). In subsequent papers [4, 5], the same authors have investigated how to report evidences of the trip even if no connectivity is available and how to implement post-payment of m-tickets. However, the authors acknowledge that their solution does not comply with anonymity and unlinkability properties.

3 Embedding Cryptographic Algorithms for Privacy

A full description of the cryptographic protocols deployed in our solution is out of the scope of this paper. However, we want to highlight that designing and implementing such a technology in a mobile phone is a challenging task. In particular, using complex cryptographic signatures are not well-suited in our context because we want to deliver anonymous credentials using a SIM card that has low computing resources. Thereafter, we sketch some problems that we had to address as well as the approaches chosen to overcome them.

Restricted resources. 2A SIM card is not powerful enough to compute group signatures or DAA. Indeed, existing schemes rely on computationally costly algebraic tools, like pairings, that are currently not available in chips like the SIM cards. Moreover, the validation of an m-ticket should not take more than 300 ms, including the interaction between devices, which strengthens the difficulty.

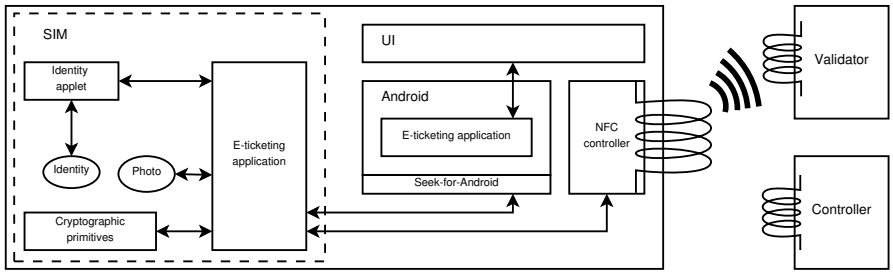

Fig. 1. Architecture of our m-ticketing application.

Revocation issues. In practice, full untraceability might be dangerous and we must address the revocation issue. For example, a manager may want to revoke a user that has lost his SIM card. Moreover, with unconditional anonymity, it becomes impossible to blacklist a SIM card that has been stolen or compromised.

In order to deal with the computational constraints, we built a cryptographic protocol that is working jointly between the SIM card and the smartphone. It is based on a group signature in which time-consuming cryptographic operations are delegated to the mobile phone. Regarding the revocation concerns, we combine the partial unlinkability property of DAA mechanisms with the blacklisting of users on the verifier side. In a DAA, signatures are linkable only if they share the same basename, a specific value included in all signatures. In our case, each basename stands for a period of time. Therefore using the same smartphone multiple times will be detected by the validation device because the SIM used the same basename multiple times. Similarly, if a cloned SIM card is deployed, the system is able to detect that the same SIM card is used several times during the same period of time. In addition to this detection, blacklists on the validation device side allow to reject some SIM cards.

4 Architecture

The proposed architecture for our m-ticketing application relies on a SIM card and an Android operating system that includes the Seek-for-Android patch as shown in Figure 1. The m-ticketing application, which is stored directly inside the SIM card, can access to the proof of personal attributes and can communicate with the NFC controller, while the application located on the smartphone memory manages the interactions with the user.

During the product registration, the m-ticketing application establishes a secure channel between the SIM card and the remote server. During this operation, the unforgeability property of the m-ticket is ensured.

During the m-ticket validation or during the travel control, a secure channel is also first established between the SIM card and the acceptance device. Afterwards, this device determines if the current m-ticket is correct, with respect to the proof of personal attributes possessed by the user as well as with respect

to the validity zones and the validity period. To realize this, the device sends a challenge and power up the NFC controller of the smartphone. Then, the SIM card returns a proof of personal information linked to the challenge in a zero-knowledge manner (*i.e*, without revealing in clear the corresponding information) using a group signature, thus achieving the data minimization principle.

Being able to realize this operation in a limited time is a challenging implementation issue. Currently, our prototype succeeds in validating the product in less than 300 ms including 150 ms that are dedicated to the communication overhead of the NFC technology. To obtain such performances, some parts of our validation protocol are delegated and precomputed by the smartphone and the final operations are done into the SIM card.

Certain types of m-ticket must incorporate a photo-ID for visual control by transport company agents of a ticket issued to a single traveler. Our solution is simple and yet provides a fair amount of privacy: the photo ID is shown on the traveler smartphone display, and a specific mechanism enforces its authenticity, based on a random mark inserted by the SIM card (which is trusted) onto the photo-ID, and verifiable by the agent.

5 Conclusion

In this paper, we have focused on the security and privacy aspects related to m-ticketing applications. More specifically, we have designed a privacy-preserving architecture for an m-ticketing application and developed a demonstrator of this application[1]. The security of the solution relies on the use of the SIM card as a secure element that enables to use anonymous, unlinkable and revocable m-tickets. The efficiency of the implementation is achieved by delegating the non-critical operations to the smartphone.

References

1. Calypso Networks Association: Calypso handbook v1.1 (2010)
2. Pirker, M., Slamanig, D.: A framework for privacy-preserving mobile payment on security enhanced arm trustzone platforms. In: Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. (2012) 1155–1160
3. Tamrakar, S., Ekberg, J.E., Asokan, N.: Identity verification schemes for public transport ticketing with nfc phones. In: Sixth ACM workshop on Scalable trusted computing. STC '11, New York, NY, USA, ACM (2011) 37–48
4. Tamrakar, S., Ekberg, J.: Tapping and Tripping with NFC. In: 6th International Conference on Trust & Trustworthy Computing. Volume 7904., London, United Kingdom, Springer Berlin / Heidelberg (2013) 115–132
5. Ekberg, J., Tamrakar, S.: Mass transit ticketing with NFC mobile phones. In Chen, L., Yung, M., Zhu, L., eds.: The Third International Conference on Trusted Systems. Volume 7222., Beijing, China, Springer Berlin / Heidelberg (2012) 48–65

[1] This work has been supported by the ANR-11-INS-0013 LYRICS Project.