Using NFC Phones for Proving Credentials

Gergely Alpár[1,2], Lejla Batina[1,3], and Roel Verdult[1]

[1] Radboud University Nijmegen, ICIS/Digital Security group
Heyendaalseweg 135, 6525 AJ Nijmegen, The Netherlands
{gergely, lejla, rverdult}@cs.ru.nl
[2] TNO Information and Communication Technology, The Netherlands
[3] K.U.Leuven ESAT/SCD-COSIC and IBBT
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
lejla.batina@esat.kuleuven.be

Abstract. In this paper we propose a new solution for mobile payments called Tap2 technology. To use it, users need only their NFC-enabled mobile phones and credentials implemented on their smart cards. An NFC device acts like a bridge between service providers and secure elements and the secure credentials (on the card) are never revealed. In this way, secure authentication can be obtained by means of anonymous credentials, implemented on a smart card to provide the functionality with minimal data disclosure. We propose to use zero-knowledge proofs based on attribute-based anonymous credentials to provide the security and privacy requirements in mobile payments. Other use cases include online shopping, easy payment, eGoverment proofs etc.

Keywords: NFC, smart phone, smart card, NFC reader, anonymous credential, zero-knowledge proofs

1 Introduction

Smart phones, smart cards and other smart devices are already omnipresent in our daily lives and used for payments, access control, transportation, etc. Especially, the ubiquity of mobile devices and the variety of services that they provide have led to many new research challenges and securing mobile communication has become essential. In addition, the necessity for cheap implementations of security protocols (due to firm constraints on area, memory, power and energy) for the applications, causes risks on security and privacy of individuals carrying the devices. As a consequence, privacy-friendly protocols are required that are also meeting (sometimes very complex) security services.

Since most mobile phones in the near future will use Near Field Communication (NFC), the importance of this technology is growing. NFC-enabled mobile phones can communicate with each other and also with other such devices, e.g. contactless cards, creating in this way an NFC-based Internet of Things.

NFC-enabled phones are used in many applications, providing links to smart posters, mobile payments, etc. All these services require secure authentication

and communication on both sides; furthermore, the threats and the capabilities of adversaries are ever increasing. Mobile payments, in particular, pose a challenge due to the requirements involved. There exist contactless payments schemes developed by Master Card, VISA, etc. These online payment applications use NFC channels as a new communication means. One disadvantage is that peer-to-peer payments are not possible. Existing online mobile payments exhibit weaknesses from both sides (the network side and the phone side) as there are simply too many things that can go wrong; especially, considering implementation issues, malware etc.

In this work we attempt to overcome the issues mentioned above. We propose to rely only on an NFC phone and a smart card to enable secure services, such as mobile banking. More precisely, because an NFC phone can also act as a reader, we separate the two by making current personal smart card readers obsolete. This setting simplifies all interesting scenarios and improves the security of the system. This is possible when applying zero-knowledge proofs with anonymous credentials to maintain strong security and privacy. In this work we explain how to use this concept for various service e.g. e-banking, online shopping, content protection, etc.

Our solution is more convenient for both, users and service providers (SP). Users are more and more aware of the importance of privacy and anonymity in digital communication and in this case there is no additional burden as their phones is all they need. A service provider, on the other hand, benefits from higher security relying on credentials (issued by the SP or a trusted authority).

In short, we advocate the transition to new authentication means. Instead of current situation in which a user has many authentication methods requiring either to carry around devices (USB token, smart card, random reader, etc.), or to remember some secret information (password, PIN), a user needs only his NFC-enabled phone to complete various security services. This way of using mobile phones as readers allows for location flexibility (i.e., mobility) for the users, which is a step forward in today's digital evolution.

1.1 Contribution

The contributions of this work are as follows:

- We propose a new solution for mobile banking as a particular example for the Tap2 technology, aiming to improve on existing solutions. In the same way, use cases of online shopping, streaming services, eGoverment applications etc. can be devised.
- We propose to use zero-knowledge proofs based on attribute-based anonymous credentials to provide the security and privacy requirements in the use cases mentioned above.
- We introduce the separation of smart card and phone. As NFC devices can act like a bridge between service providers and secure elements, it is reasonable to maintain credentials in a secure environment to avoid them to

be revealed. Only proofs about these credentials (e.g., attributes, ownership, etc.) are revealed upon a legitimate request. NFC phones, having more computational and memory resources, are suitable platforms to implement complex protocols behind anonymous credential. This enables to implement stronger security for less.
– This separation leads also to a more unified approach in terms of modularity. By joining forces of a powerful mobile device and a tamper-resistant smart card, not only is secure authentication (identity proof) possible, but also more fine-grained proofs. Anonymous credentials, implemented on a smart card, provide functionalities to prove qualities of the credential as well as its owner with high security assurance and minimal data disclosure.

1.2 Outline

The remainder of this paper is organized as follows. In Sect. 2 we give basic information about NFC technology and we mention some related work on NFC solutions, i.e. protocols and their security issues. In addition, we also describe an existing e-banking solution and we outline necessary cryptographic concept implied by our proposal. The model for our solution is detailed in Sect. 3. Our new solution called Tap2 technology is introduced in Sect. 4 and one of its possible use cases (i.e., mobile banking) is explained in Sect. 5. Section 6 briefly explains possible threats and attacks. Section 7 concludes this paper and suggests some alleys for future research.

2 Background

There are various protocols that could be improved, in terms of security and usability, by using NFC technology. However, in order to limit the scope of this paper we apply our generic credential proving method only on payment services. In this section we first introduce the NFC features and technology and secondly we describe an e-banking solution that is frequently used in Europe to perform on-line financial transactions. We also introduce our model notation and describe the protocol we aim at improving. In addition, we summarize the cryptographic concepts we use as the main building blocks of our model.

2.1 Technology

The Near Field Communication (NFC) technology is an extension of several Radio Frequency IDentification (RFID) proximity communication standards [12, 11, 17]. It basically combines the high frequency (13.56 MHz) RFID standards and reformulates them adding some more features into two new communication standards [13, 14]. The two main new features added in these standards are peer-to-peer connections between two active NFC devices (NFCIP) and the emulation of a passive proximity RFID tag. The initial goal behind NFC technology is to establish more complex wireless channels that operate at a proximity distance.

This makes NFC much more ambitious than RFID systems. The latter is limited to plain identification, tracking of unique card numbers or storing small monetary values in the memory of an RFID tag. Because NFC is backwards compatible to RFID systems, several deployed devices could be accessed by an NFC-enabled device. These include electronic passports and identity cards based on the ICAO standard [10], most contactless public transport tickets, and access control tags that operate at 13.56 MHz.

While RFID standards were merely focused on specification of the modulation, encoding, start and stop conditions of the communication, NFC extends its specification by adding application formats [23, 20, 22, 21] and integration of (multiple) secure elements [6, 5, 16, 15]. Secure elements are comparable with regular smart cards and are available in many forms, e.g. contactless smart card, Universal Integrated Circuit Card (UICC), MicroSD card with RF interface or an internal embedded chip which is integrated into an NFC controller chip. The latter one is used in the popular Google Nexus S phone a long side UICC that contains the Subscriber Identity Module (SIM) and is supplied by the users telephone company.

Since the introduction of NFC technology, a number of protocols have been proposed [4, 24, 28, 1, 9] for specific applications. None of these protocols generalizes and uses the technology in such a way that only the essential security requirements are addressed to prove a credential. A more generic approach could be used for most applications without redesigning the original protocol. There are several security issues found in drafts of the standards and in early prototypes of NFC-enabled devices related to NFC [19, 29, 26]. These papers address weak spots in rapidly built systems and protocols which have not been carefully tested or formally proved.

2.2 E-Banking

Current payment solutions use complex security protocols to authenticate, verify and approve credentials. Service providers, such as banks, often use the most progressive protocols to circumvent fraudulent transactions. This paper therefore proposes the use of NFC technology in the widely deployed on-line banking solution based on the EMV Chip Authentication Program (CAP). EMV-CAP was introduced by Mastercard International in 2004 to proof possession of a set credentials by the user. These credentials include the smart card and the PIN code corresponding to the bank account of the user.

E-banking protocols often make use of a second secure channel provided by a dedicated smart card and a reader which are deployed by the bank itself. These protocols heavily depend on complex cryptographic calculations performed by the smart card. The smart cards and readers are made of tamper resistant hardware to provide a trusted infrastructure at the consumers side. Protocols like these are considered more secure because of their two-factor authentication (smart card and PIN code) and their strict secure channel separation between on-line (internet) and off-line (smart card and reader). The downside of using a separate smart card and reader is the extra user interaction that is required for

each transaction. We present the required steps in a model of the EMV-CAP protocol in Figure 1, it is currently used by several European banks such as Barclays, RBS, ABN AMRO, Rabobank, KBC, and Nordea.

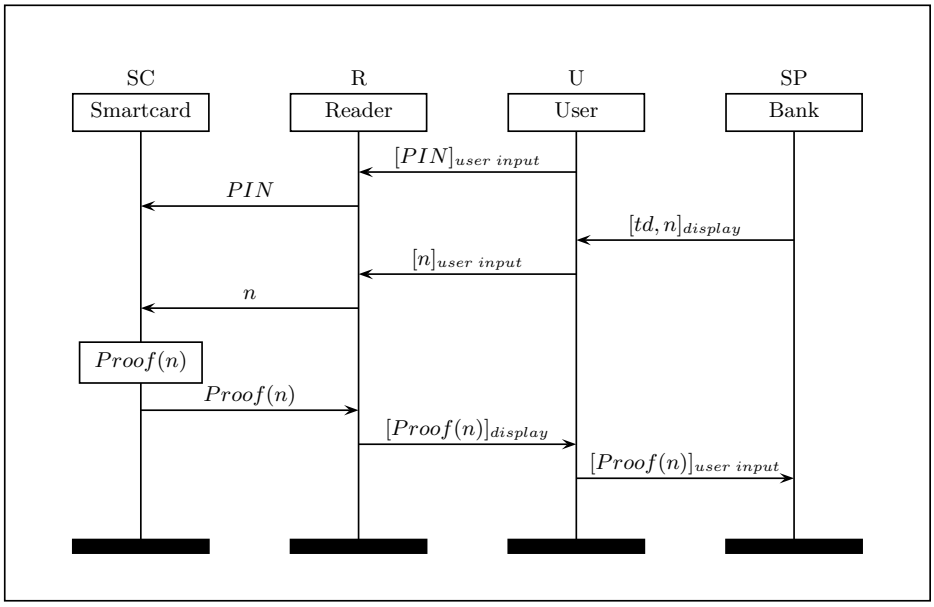

Fig. 1. Protocol used by EMV CAP

What immediately strikes us in Figure 1 is the fact that the transaction details td are not signed by the smart card. They are shown to the user, but not included in the proof that is generated by the smart card. Some banks provide an optional extra user input after entering the nonce n when transferring a large amount of money. This however, increases the amount of user interactions that take place during the transaction and makes it less attractive to use for regular transactions. Since this extra user input is used only occasionally, we discard this as part of the protocol. More details about this protocol is available under a non-disclosure agreement with Mastercard, but most of its operations are reverse engineered and published by Drimer et al [3].

2.3 Cryptographic concepts

Smart cards are reasonably cheap hardware devices that provide tamper resistance for secret keys and are equipped to perform cryptographic computations. As smart cards are prevalent, convenient for users, and clear links to distinct services, they are expected to remain dominant for the foreseeable future. Smart

cards are not only able to support traditional public-key infrastructures (PKIs), but also more complex cryptographic protocols.

A *zero-knowledge (ZK) proof* is the most important example for such a cryptographic technique for achieving privacy and security at the same time. A ZK protocol is a challenge–response algorithm that enables a prover to convince a verifier of the validity of a statement without releasing any knowledge beyond the validity of the statement. While an *interactive* ZK proof requires the presence of both participants in the course of the protocol, a *non-interactive* ZK proof can be generated by the prover alone. Interactive proof protocols can be changed into non-interactive ones by applying Fiat–Shamir heuristic [7], that is, substituting the verifier's random challenge by cryptographic hashing. Extending the input of the hash function by a message, a non-interactive proof of the knowledge of a secret value (such as a private key) can be transformed into a digital signature.

An *anonymous credential* is a credential, a signed data structure by a trusted issuing authority, that reveals no information about the identity of the owner. In order to verify a credential, the verifier is supposed to know the public key of the issuer. The most important anonymous credential technologies, such as U-Prove [25] and Idemix [27], allow for signing several attributes in a credential. While a basic ZK proof demonstrates merely the fact of owning a credential signed by a certain issuer (e.g., "I have a driving license"), in case of selective disclosure, a user can reveal some attributes too (e.g., "I have a driving license which is due to expire on 12–Dec–2012"). The most advanced functionality of an anonymous credential enables credential owners to provide property proofs about the attributes (e.g., "I have a driving license which is still valid (i.e., today $\leq$ expiry day) and the card is not revoked (i.e., the card number is not on the revocation list)"). Note that the identity of the prover is not revealed in these examples.

Zero-knowledge proofs and anonymous credentials are important building blocks in applications to achieve privacy for the users (provers) as well as security for the service providers (verifiers). Since wireless technologies are susceptible to be eavesdropped and to man-in-the-middle attacks, these techniques play essential roles to prevent information leakage.

To summarize, smart cards are ideal means for the construction of privacy-friendly and secure protocols by carrying anonymous credentials and delivering zero-knowledge proofs about attributes.

3 Model

In this section we define our model and we specify the security requirements of our system.

3.1 Participants

In our model a user U is a human being who is assumed to have an NFC-enabled mobile phone and a smart card SC. A smart card carries an anonymous

credential issued by a trusted issuing authority IP. Although a user can have several smart cards in practice, we assume only one smart card in a protocol run. A mobile phone has two states:

- When it is in *normal mode*, the mobile phone is denoted by M. Though it provides full functionality, it is untrusted, e.g., prone to be infected by malware.
- In order to carry out security sensitive tasks, U can switch the mobile phone to its *trusted mode*, denoted by TM.

In a protocol, a user, employing his hardware devices, is required by a service provider SP to prove some statement. The credential contains a secret key and further attributes, signed by IP, that enables the user to construct the expected proof. In Table 1 all the participants with corresponding abbreviations are given.

Table 1. Participants.

U	User
SC	Tamper-resistant smart card with a credential
M	NFC-enabled mobile phone in normal mode
TM	NFC-enabled mobile phone in trusted mode
SP	Service provider
IP	(implicitly) Trusted authority issuing credentials

3.2 Security requirements

Here we elaborate on the security requirements that we assume or wish to obtain. As mentioned above we aim at privacy-friendly solutions meeting the security requirements. Therefore, we need a substantial computational power but considering the trends with mobile phones, this seems to be easily accessible. In addition, as mobile devices are becoming more and more powerful, it is reasonable to assume that individuals will want to carry out most tasks on them instead of desktop computers. On the other hand, mobile devices, especially when representing more and more value, are vulnerable to theft. For this purpose, we envision an intuitive, new technology, the *trusted mode* of mobile devices. A user should be able to switch a mobile phone between trusted and normal modes using a hardware button. When in trusted mode, not only does the phone restrict its set of functionalities, but it also changes its appearance. A mobile phone in trusted mode, while emitting some distinct visual sign, can only communicate through NFC, while it has internal access only to a trusted domain (such as a secure element), that allows cryptographic computations and secure storage. Note that no software means may switch between modes and the visual sign must be out of reach of other hardware or software elements.

To summarize, our model assumes/implies the following concepts:

– Secure and privacy-preserving authentication method for the user
– Reliable information about the user for the SP issued by a trusted authority (IP) (because of the credential)
– Credentials never leave the smart card, only the proof of ownership (and possibly some knowledge on attributes) about the credential. In other words, we assume selective disclosure of attributes and property proofs of the attributes i.e. the use of attribute-based anonymous credentials; such as U-Prove [25] or Idemix [27].
– The authentication is only possible if both the user and the smart card are present.
– The service provider obtains reliable information about the user (it is not the case for a password authentication)
– In the case of loss or theft of a mobile phone or a smart card, no unauthorized parties should be able to gain access to the users' credentials or authenticate on their behalf.
– The smart card is assumed to be tamper-resistant and the attacks aiming the key-recovery using side-channel information such as power consumption [18] or electromagnetic emanations of the device are out of the scope of this paper.

Considering the issue of trust in mobile phones we assume the following for the resulting protocols:

– If the mobile phone is trusted, it can act simply as a card reader. We foresee that several smart cards will stay separated from the mobile phone, such as bank and credit cards, identity card, driving license, etc. In order for it not to be able to store any valuable information about the credentials, smart cards should communicate only proofs about the credentials and attributes. (Note however, that the information might be stored that the smart card has ever proven.)
– If the mobile phone is partially trusted, limited permissions can be provided; such as ABN-AMRO's app[4]in which a separate PIN code has to be used (not the one on the card) and only read-only account information and transfers to own accounts are allowed.
– If the mobile phone is assumed to be prone to get infected by malicious software, we propose a trusted state for mobile phones. In this trusted state a phone has restricted access to its own resources: It can use NFC functionality, perform cryptographic computations, and take secure input.
– Another solution can be the inclusion of a secure element which is out of the scope of this work.

4 Tap2 technology

In [2] the Snap2 user-friendly technology has been designed for authentication and payment methods to web applications. A QR code (a two-dimensional bar-

[4] http://www.abnamro.nl/en/prive/slimbankieren/mobiel-bankieren/introduction.html

code), containing channel information, is generated by the service provider's web server and scanned by the user's mobile phone. Using the information, the mobile phone can generate an authentication (or a payment) and send it to the web server through the Internet.

Referring to the similarity and the differences, we call our technology Tap2. A Tap2 scheme includes the participants described in Table 1, and it requires the user to have his/her mobile phone and the relevant smart card present. A user can perform fundamental proofs, see Table 2, by letting the mobile phone and the smart card to communicate through NFC and switching the mobile phone to the trusted mode for sensitive tasks such as, entering a PIN code.

Table 2. Types of proofs.

Abbreviation	**Type**	**Components**
CRED	Owning credential	signature
ID	Having certain identity	identifiable attributes
PROP	Having some characteristics	attributes and/or attribute properties
APPR	Approval	proof from above and authentic consent

A smart card SC contains an attribute-based anonymous credential and the logic that is required to the following proofs. To prove that a credential is present, SC generates a signature on a given nonce, based on the proof of knowledge of the corresponding secret key.

If identification is required, the SC selectively discloses an identifying attribute (or an identifying set of attributes), and proves that it is indeed in the credential. This proof implicitly contains the credential itself. Similarly, a property proof also inherently proves the knowledge of an anonymous credential's secret key; however, the proof contains zero-knowledge subproofs about some properties of attributes. Finally, an approval is any proof from the ones above augmented by the user's approval of a transaction. Figure 2 shows the dependencies of these proofs on each other and on the participants.

5 Applications

5.1 A use case: Mobile banking

On-line banking is carried out with two-factor authentication and transaction approval; besides a password authentication, a second means is applied. A temporary one-time password generated by either the bank and sent by e-mail or sms, or the on-line banking card reader at the user.

Our scheme (see Figure 3) is highly secure, yet simple and intuitive for the user without an additional special device or network channel. Since there is much interaction between the card and the mobile phone, the simplest way for a user is to place the phone on the bank card and follow the instructions. However, the

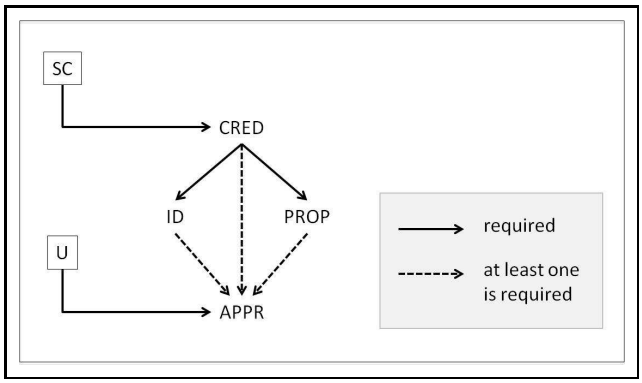

Fig. 2. Dependencies of proofs.

user has to pay attention to enter the PIN code only when the mobile device is in trusted mode (TM).

A money transfer transaction in the mobile banking application works as follows from the user's point of view:

1. After the user prepares a money transfer and sends it to the server, the server requests an authorized approval, that is, the user's consent and a proof that the authentic user and the required bank card are present. The request contains all transaction details td, information about the transfer and the bank's signature on it, and a nonce n. The variables are communicated to the mobile phone through the Internet and to the smart card through NFC.
2. The smart card verifies the bank's signature in td. The mobile phone displays an alert to the user to switch the device into its trusted mode.
3. Having switched M to TM, the user gets the relevant information about the transfer on the mobile phone: bank, account numbers and amount. To approve the transaction, the user enters his PIN on the mobile phone, which is communicated to the smart card through NFC.
4. While the user switches back to M (normal mode), the smart card signs td as a proof of approval. The proof is sent to the bank's server through the mobile device.

Transaction details td play an essential role in the protocol. They show the identity of the bank and the description of the transaction (e.g., in case of a money transfer: `bank account from`, `bank account to`, `sum`). The same tuple td should be used to display information to the user and to be input to the smart card.

The user has important roles to provide authenticity and security. Firstly, the user has to switch his mobile phone to its trusted state for the most sensitive tasks. Secondly, receiving the transaction details, he has to approve the transaction by providing his PIN code. Finally, he has to switch the phone back

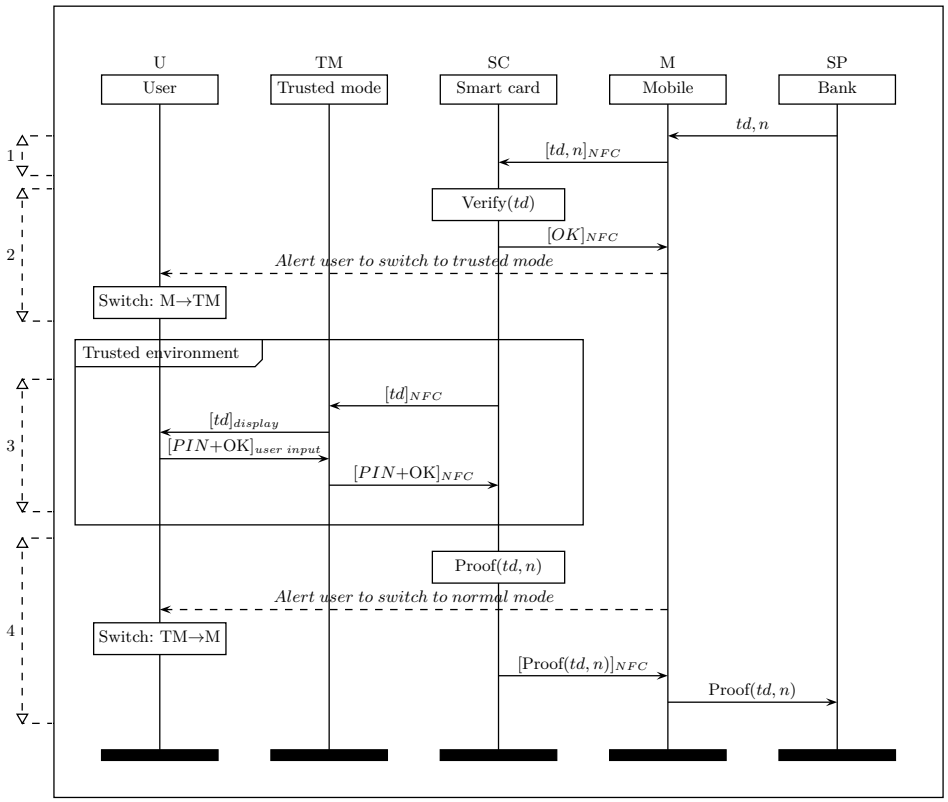

Fig. 3. E-Banking Scheme

to its normal state for it to be able to connect to the bank's server through the Internet and to send the proof signature from the card to the server.

5.2 Other applications

Next we show a list of examples including the classification that point out which features of the protocol could be used.

- **Pay the bill**
  We assume that an invoice is equipped with an NFC tag that contains a prepared payment transaction to the provider's bank account. By tapping the tag first and then a bank card, a user can approve the transaction with a mobile phone using the credentials from the bank. For financial transactions it is preferred to use trusted mode.
- **Peer-to-peer payment**
  User A prepares a signed statement with the transaction details on the mo-

bile phone. By tapping A's device and B's bank card, B can approve a transaction. The security requirements are similar to those of Pay the bill.
- **eGovernment identity proofs**
  To prove the identity a user may decide not to switch to trusted mode. There is no secret information entered by the user, the identity card provides the zero-knowledge credential proof and the user only has to actively bridge the credential to the service provider (e.g. for customs declaration).
- **Ordering cigarettes from a vending machine**
  An identity card could also be used to provide a proof that a user is old enough to buy cigarettes. For such a simple proof, the user could ignore trusted mode as well as confirmation. It leaks hardly any detail about the users privacy.

6 Threat analysis

In this section we briefly consider the threats that apply and that we aim to protect against. Our solution is intended to protect against the following attacks.

- Phishing: An attacker that aims at online phishing attacks would fail because there is no PC involved, such as in other options using e.g. SSL.
- Relay attacks such as described by Francis et al. [8] apply when assuming that NFC can be eavesdropped or even changed [8]. However, an attacker cannot generate a valid proof without knowing the credentials on the smart card.
- In the case of phone or smart card theft or loss, the fact that there are two devices required for authentication somewhat reduces the risks. In addition, if a phone is stolen or lost, the Tap2 can require the authentication of a user. If this fails, the phone is locked. Also, if a phone is lost, users can revoke Tap2 credentials from SP. The same applies for a smart card loss.
- Malware on phones is probably the most serious threat that should be solved in general so we do not consider it specifically in this work.
- Implementation or physical attacks using a side-channel such as power consumption or EM are out of the scope of this paper, as mentioned above.

7 Conclusions and Future work

A new solution for mobile payments called Tap2 technology is proposed in this work that requires from users only their NFC-enabled mobile phones and credentials implemented on their smart cards. Secure authentication (proof) is obtained by means of anonymous credentials implemented on a smart card to provide the functionality with minimal data disclosure. The idea can be extended to other use cases such as online shopping, streaming service, eGoverment proofs etc.

For future work, it would be interesting to incorporate a mobile trusted module (secure element) in the protocols. An interesting research direction is to investigate possible integration of open technologies, such as OpenID, in this

context. Another natural extension considering Idemix possibilities, (to handle more anonymous credentials with the same master key of the user), is to include more smart cards into one protocol.

8 Acknowledgement

This work was supported in part by the European Commission under contract number ICT-2007-216676 ECRYPT NoE phase II and by the research programme Sentinels as project Mobile IDM (10522). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.

References

1. W. Chen, G.P. Hancke, K.E. Mayes, Y. Lien, and J.-H. Chiu. NFC Mobile Transactions and Authentication Based on GSM Network. *Near Field Communication, International Workshop on*, 0:83–89, 2010.
2. Ben Dodson, Debangsu Sengupta, Dan Boneh, and Monica S. Lam. Secure, Consumer-Friendly Web Authentication and Payments with a Phone. In *Conference on Mobile Computing, Applications, and Services (MobiCASE'10), Santa Clara, CA, USA*, 2010.
3. Saar Drimer, Steven J. Murdoch, and Ross J. Anderson. Optimised to fail: Card readers for online banking. In *Financial Cryptography*, pages 184–200, 2009.
4. Sebastian Dunnebeil, Felix Kobler, Philip Koene, Jan Marco Leimeister, and Helmut Krcmar. Encrypted NFC Emergency Tags Based on the German Telematics Infrastructure. *Near Field Communication, International Workshop on*, 0:50–55, 2011.
5. Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) (ETSI TS 102 613), 2008.
6. Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (ETSI TS 102 613), 2011.
7. Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *CRYPTO*, pages 186–194. LNCS, 1986.
8. Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical NFC Peer-to-Peer Relay Attack using Mobile Phones. IACR e-print archive, April 2010.
9. Van Dam Gauthier, Karel M. Wouters, Hakan Karahan, and Bart Preneel. Offline NFC payments with electronic vouchers. In *Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds*, MobiHeld '09, pages 25–30, New York, NY, USA, 2009. ACM.
10. Machine readable travel documents, 2003.
11. Identification cards — contactless integrated circuit(s) cards — vicinity cards (ISO/IEC 15693), 2000.
12. Identification cards — contactless integrated circuit cards — proximity cards (ISO/IEC 14443), 2001.
13. Information technology — telecommunications and information exchange between systems — near field communication interface and protocol 1 (NFCIP-1) (ISO/IEC 18092), 2004.

14. Information technology — telecommunications and information exchange between systems — near field communication interface and protocol 2 (NFCIP-2) (ISO/IEC 21481), 2005.
15. Information technology — telecommunications and information exchange between systems — near field communication wired interface (NFC-WI) (ISO/IEC 28361), 2007.
16. Information technology — telecommunications and information exchange between systems — front-end configuration command for NFC-WI (NFC-FEC) (ISO/IEC 16353), 2011.
17. Specification of implementation for integrated circuit(s) cards (JICSAP/JSA jis x 6319), 2005.
18. P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology: Proceedings of CRYPTO'99*, number 1666 in Lecture Notes in Computer Science, pages 388–397. Springer-Verlag, 1999.
19. C. Mulliner. Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. In *Proceedings of the 1st International Workshop on Sensor Security (IWSS) at ARES*, pages 695–700, Fukuoka, Japan, March 2009.
20. Technical Specification, NFC Data Exchange Format (NDEF), 2006. NDEF 1.0.
21. Technical Specification, NFC Record Type Definition (RTD), 2006. RTD 1.0.
22. Technical specification, connection handover, 2010. Connection Handover 1.2.
23. Technical Specification, Smart Poster Record Type Definition, 2006.
24. Charl A. Opperman and Gerhard P. Hancke. A Generic NFC-enabled Measurement System for Remote Monitoring and Control of Client-side Equipment. *Near Field Communication, International Workshop on*, 0:44–49, 2011.
25. Christian Paquin. U-Prove Cryptographic Specification V1.1. Technical report, Microsoft, Available: https://connect.microsoft.com/site1188/Downloads, February 2011.
26. Michael Roland, Josef Langer, and Josef Scharinger. Security Vulnerabilities of the NDEF Signature Record Type. *Near Field Communication, International Workshop on*, 0:65–70, 2011.
27. IBM Research Zürich Security Team. Specification of the Identity Mixer Cryptographic Library, version 2.3.3. Technical report, IBM Research, Zürich, Available: https://prime.inf.tu-dresden.de/idemix/, June 2011.
28. Rainer Steffen, Jorg Preissinger, Tobias Schollermann, Armin Muller, and Ingo Schnabel. Near Field Communication (NFC) in an Automotive Environment. *Near Field Communication, International Workshop on*, 0:15–20, 2010.
29. Roel Verdult and Francois Kooman. Practical attacks on nfc enabled cell phones. *Near Field Communication, International Workshop on*, 0:77–82, 2011.