Position Paper

November 08

Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID)

www.enisa.europa.eu

Version: 1.0.1 (final)
Date: 2008-11-21

Editors: **Ingo Naumann, Giles Hogben**
European Network and Information Security Agency (ENISA)
E-Mail: eid@enisa.europa.eu

Contributors:

Raúl Benito, Isdefe, Spain
Roger Dean, EEMA, Belgium
Lothar Fritsch, Norwegian Computing Center, Norway
Jonathon Gould, Asia-Pacific Connections Pte Ltd, Singapore
Jaap-Henk Hoepman, TNO and Radboud University Nijmegen, The Netherlands
Steve Lazar, Texas Instruments, USA
Herbert Leitold, Zentrum für sichere Informationstechnologie Austria (A-SIT), Austria
Greg Pote, Asia Pacific Smart Card Association (APSCA), China
Heiko Roßnagel, Fraunhofer Institute for Industrial Engineering (IAO), Germany
Arnim von Schwedler, Judge, 9 Senat Gericht, Berlin, Brandenburg, Germany
Daniele Vitali, Reply, Italy
Frank Zimmermann, Hewlett-Packard, Switzerland
André Årnes, Oracle Norway / NISlab, Gjøvik University College, Norway

Group members participate as individuals. This paper should therefore not be taken as representing the views of any company or other organisation, and does not in any way bind group members when dealing with the issues it covers in other contexts.

Executive Summary

Mobile devices, like smart phones and PDAs, will play an increasingly important role in the digital environment [8]. Besides their primary use, these devices offer, based on the security features of their secure elements, the possibility to electronically authenticate their owners to a service. In the near future we might use our phone to pay our taxes, buy metro tickets, elect a president, play the lottery or open bank accounts. With Hong Kong, Singapore and Taipei being 'the most mobile-penetrated territories on the planet' [16], the Asian region in particular is experiencing growing demand for these services. A main driver in the Asian market is the consumer's interest in convenient solutions which are easy-to-use and involve as few devices as possible. In Europe, enhanced security might become a second incentive for these technologies. Mobile devices can act as a user-interface for online applications and in this way act as a secure, secondary authentication channel.

However, as is the case with many new technologies, the pervasive use of mobile devices also brings new security and privacy risks. Persons who make extensive use of mobile devices continuously leave traces of their identities and transactions, sometimes even by just carrying the devices around in their pockets. Statistics show an increase in the theft of mobile devices [19] which nowadays store more and more personal information about their users. Although the secure elements (based on smart card technology) are very suitable for storing data, vulnerabilities do exist and new weaknesses might be discovered. Due to the increasing complexity of mobile devices, they are now prone to attacks which previously only applied to desktop PCs. BitDefender lists the exploitation of mobile device vulnerabilities three times among the top ten 'e-Threats' for 2008. According to the *E-Threats Landscape Report*, mobile devices are about to be increasingly targeted by new virus generations because of their permanent connectivity. Classical scam methods using SMS are expected to rise in parallel [3]. Therefore the original notion of seeing the mobile device as a personally, trusted and trustworthy device needs to be re-evaluated.

Throughout this paper we will look at different use-cases for electronic authentication using mobile devices. We will identify the security risks which need to be overcome, give an opinion about their relevance, and present mechanisms that help in mitigating these risks. Furthermore, we will look at use-cases where mobile devices even act as a security-enhancing element by providing an out-of-band channel or a trustworthy display.

Mobile devices have an enormous potential. Many new electronic services are currently being developed and tested and many of them are likely to find customer acceptance because of the opportunities and benefits they offer. We strongly believe that, if these new technologies are applied in the right way, they also constitute a big opportunity when it comes to the secure, sophisticated authentication mechanisms needed for future applications.

Introduction

ENISA Position Papers represent expert opinion on important NIS topics. They are produced by a group selected for their expertise in the area. The content of this paper was collected and discussed between March and December 2008 via wiki, mailing list and telephone conferences, and was edited by ENISA. The final version has been reviewed by the people listed above.

This paper aims to provide a useful introduction to security issues in the area of electronic authentication using mobile devices and highlights the most important threats. Examples are given throughout the paper. The examples provided are not necessarily those most representative or important, nor is it the aim of this paper to conduct any kind of market survey.

Audience

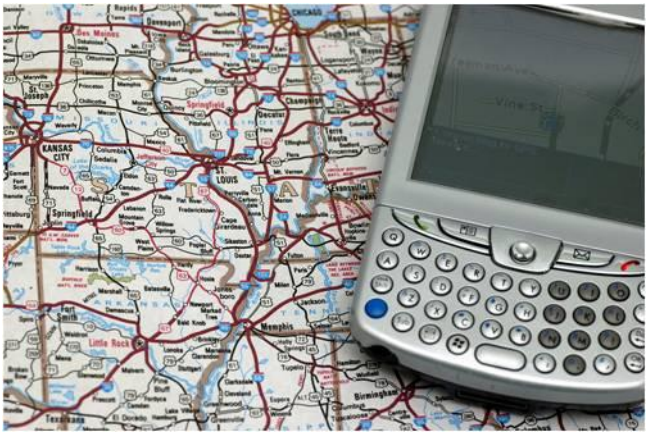
This paper is aimed at corporate and political decision-makers as well as providers of mobile applications. It also seeks to raise awareness among political and corporate decision-makers of the legal and social implications of new developments in certain mobile technologies. In particular, the findings should have important implications for data protection and security policies.

Table of Contents

A Future World

Ola Nordmann uses his smartphone as his principal communication and interaction device for all electronic communication. He is frequently authenticating to a number of services every day:

- On the way to work, Ola taps his phone against a terminal at the metro entrances gates which gives him access to the station. While in a train, he sends invitations to two friends for a concert that same evening via SMS. His friends reply and Ola downloads and pays for three online tickets for the concert.
- At work, Ola enters a PIN code, thereby switching the phone to 'work mode'. Now, outgoing calls are booked to his work phone account, but incoming calls and messages from the private domain are still received. He opens the door to his office by simply waving the phone towards the door which automatically logs him into the computer system.
- Ola is an officer with statutory authority in his company. Today he has to open a new bank account for his company which requires identification using a government-issued ID document and documented evidence of his authority. Since his phone has a built-in ID card functionality he can identify and authenticate himself online to the bank and does not have to leave the office for this procedure.



- Later on, he electronically signs a contract with one of his company's clients which he has received by e-mail.
- After work, Ola goes home, switches the phone to private mode, and gets ready to go to the concert with his friends. They meet in a nearby bar which he identified as meeting their profile using a location-based service. Ola transfers their tickets to their smartphones using Bluetooth or Near Field Communication (NFC), whereby the ticketing software ensures that Ola is not a black market ticket dealer.
- At the concert location, the friends buy each other drinks, paying for them with their phones via NFC. The barkeeper verifies their legal drinking age using information provided by their mobile phones. Later on, they submit their votes for a musician contest and, with that, automatically participate in a lottery.

Quick Technology Review

A mobile phone (or cellular phone) is a portable electronic device primarily used for voice communication over a network of base stations. Besides the standard voice function, mobile phones may provide many additional services, such as SMS (text messaging), MMS (photo messaging), email, taking pictures with an integrated camera, access to the Internet, and games. A slightly different kind of mobile device is the 'personal digital assistant' (PDA), also known as a palmtop computer, which usually has a bigger colour screen and a keyboard or a touch screen which allows the user to enter longer texts more conveniently. Like mobile phones, PDAs might be used as media players and can access the Internet via Wi-Fi or wireless wide-area networks. In the following, we will refer to mobile phones and PDAs as 'mobile devices'.

A very important feature of mobile devices is the short message service (SMS) which permits the transmission of short text messages to another mobile device. Increasingly, text messages are also used as a (secondary) authentication channel (eg, online banking) or for the confirmation of payments.

Whenever secret keys have to be securely stored, smart cards usually come into play[1]. A smart card is generally a thin plastic card with an integrated circuit where information can be stored. Depending on the chip technology, the smart card just acts as a simple memory or it can perform complex operations such as communicating via secure channels or digitally signing files. A major advantage is that even inexpensive smart cards can have a highly secure memory where secret keys or other sensitive information can be stored. A smart card derives its security from the fact that it is either tamperproof or tamper evident: any attempt to retrieve the secrets on the card by physical means will either erase all the data on the card or be clearly visible from the outside of the card. The communication to the reader can take place either via electrical contacts (as defined in ISO 7816) or via a contactless RF interface (ISO 14443 or other).

Radio Frequency Identification (RFID) tags, contactless smart cards and NFC devices are closely related technologies that are sometimes confused. An RFID tag can be active or passive depending on whether the tag has an internal power source. There is a wide variety of specified ranges, from about 10cm up to 200m, as well as computational power, depending on the technology. Simple low-cost tags just transmit a fixed number. These RFID tags typically have no security features whatsoever[2].
On the other hand, both contactless smart cards and NFC devices can perform complicated cryptographic operations. An NFC communication[3] can be established either between a

[1] However, there are already a number of mobile handsets in the design phase which will take a microSD card instead.

[2] There are two EPC standards: EPC gen 2 which is a UHF based standard. Soon to be ratified is the EPC HF standard which uses the Gen 2 protocol but with the air interface at 13.56 MHZ (versus 860-960 MHZ for UHF).

[3] NFC is based on the ISO 14443 proximity-card standard.

passive contactless smart card and an active reader or between two readers. NFC readers can be built into mobile devices, such as mobile phones. However, the radiofrequency communication between a mobile device and another mobile or reader device or RFID tag may not necessarily be based on NFC communication. NFC is a standard built upon existing contactless protocols ISO14443A, FeliCa and ISO14443B.

While it looks highly likely that all mobile devices will eventually use the NFC standard for contactless communication, there are nevertheless over 40 million mobile devices in Japan with contactless communication based on FeliCa only (and not NFC). With the current lack of NFC mobile phones, there are also a number of pilots based on some type of mobile contactless protocol (usually ISO14443) without full NFC compatibility. These 'transitional' mobile contactless technologies are likely to persist while the shortage of NFC mobile phones continues. Another short-range communication technology which has recently been integrated into mobile phones is Bluetooth (which will not be covered by this paper).

Mobile devices can be used to pay for goods or services. In this report, we distinguish between 'SMS Payments' and 'NFC Payments', depending on the technology required for the payment[4]. In order to carry out an NFC payment, the consumer is usually only required to place their mobile device on the merchant's reading device. We speak of SMS payment when the transaction implies sending or receiving an SMS[5].

Mobile devices can communicate through open networks, such as the Internet, closed networks, such as mobile networks, and also Bluetooth networks which might be open or closed. It should be noted that mobile devices may connect to the Internet indirectly, through a mobile operator network with a gateway to the Internet, or directly through Wi-Fi and (in future) WiMAX networks. In the future an increasing number of mobile devices will be able to communicate through contactless or NFC protocols with a wide variety of proprietary networks (eg, bank payment and transit payments networks), with other mobile devices, and even with single passive RFID tags.

Usually, a mobile device needs a 'secure element' (SE) where private or secret keys are stored. The Mobey Forum identifies three categories of SEs: removable hardware, non-removable hardware, and software [18]. Depending on the category, the SE could therefore be the mobile device's memory or an internal card such as a Universal Integrated Circuit Card (UICC), containing the Subscriber Identity Module (SIM) application, or an SD or microSD card[6].

---

[4] This report does not cover all available technologies. A possible classification could be to distinguish between 'remote' and 'proximity' payments. The former implies the use of SMS/USSD/Packet Data and the fact that the payment information is processed remotely; the latter implies the use of NFC technologies (or similar).

[5] The consumer could, of course, also use a regular wireless Internet connection with his mobile device to perform a financial transaction. This case is outside the scope of this paper.

[6] How separate eID cards (even contactless cards) could serve as secure elements is an idea that is also being discussed within the community.

Mobile Devices as Security Tools

Phishing websites, rogue websites that invite bank customers to enter their passwords or other credentials, are constantly attacking online banking applications. Even though bogus websites normally cannot provide valid HTTPS certificates, the users very often do not check whether the connection is encrypted (yellow URL bar) or they accept unknown certificates. The next set of attacks involves sophisticated malware which compromises the browser and then replaces URLs, payment transactions or bank account numbers. In online banking, customers often have to provide a transaction authentication number (TAN) or a temporary PIN (received by SMS or generated by some other security token [14]) in order to clear a financial transaction[7]. Other countermeasures involve the use of physical tokens which have to be connected directly to the user's computer in order to authorize a transaction, usually smart cards. Provided these systems are well designed, they actually can eliminate the phishing threat completely.

! **Thus, besides the convenience mobile devices might provide us with in our daily life, they could also serve as tools to improve the security of already existing applications.**

Another example, also described as a use-case below (*see* Electronic Signature with Mobile Device (Trustworthy Viewing), page 16), is an electronic signature application. A mobile device might provide the trustworthy display that enables the user to verify the document to be signed.

[7] How well these mechanisms actually address the phishing threat depends heavily on the details. For example, whereas a regular TAN does not provide any protection against phishing attacks, the slightly more complicated concept of indexed TANs (iTANs [21][26]), where the bank requires the user to provide a particular TAN out of a list of 100, forces the attacker to connect to the bank before the TAN expires, usually within a couple of minutes. Thus, a successful attacker has to perform a real-time man-in-the-middle-attack which is considerably more difficult than just collecting passwords and TANs over a period of some days and then running the exploits within a short time frame. Even more protection is required against malware that attacks the browser directly. In this case, the real site is connected to the real user, but the browser-in-the-middle (as this type of attack is called) can modify bank account numbers and transaction amounts at will. Sophisticated malware will automatically delete all traces including the software itself. A possible protective measure in this case is to include amount and beneficiary in the message requesting a TAN code, and to send this message over a secondary channel not involving the browser at all.

Security Issues (Risks)

We define 'security risk' as follows:

! **A security risk is the potential that a given threat will exploit the system's vulnerabilities. It is measured by the impact multiplied by the probability of the threat [10].**

Assets

Most of the assets (the 'What has to be protected?') remain the same across all use-cases. The main categories of asset are:

- Sensitive/personal Information

Sensitive information stored on mobile devices or in background databases has to be protected. We refer to sensitive information in a broader sense here, ie, any kind of personal information (eg, name, date of birth), including biometric identifiers (eg, facial image, fingerprints), as well as credentials (eg, secret keys) and information about location. Location privacy is a particularly important issue here because mobile devices constantly communicate with their environment which might allow tracking of the user's movements. The background systems contain personal information as well: transaction log files, passenger profiles and the like, which, even if not directly linked to specific persons, could infringe the privacy of the users.

- Access to bank accounts/money

The access to a bank account constitutes an asset independent of the account holder's personal information: a successful attack on a bank account, in particular the illicit transfer of money to another account via a phishing site, could be performed without the attacker actually learning the account holder's personal information or access credentials. However, usually such an attack also involves the theft of personal information.

- Access to physical goods, personal property or buildings

Since a mobile device can also grant access to buildings or physical goods, eg, via vending machines, this constitutes another asset. By its nature a mobile device too is an asset, small enough to be most easily stolen or lost.

- Service availability

In addition to all this, the availability of the service can be considered an asset. Other assets which are specific to one of the use-cases are mentioned in the corresponding section about this use-case.

Vulnerabilities

In this section we will explore the vulnerabilities of mobile devices and, in particular, the vulnerabilities of smart cards and NFC/contactless devices, in order to understand the security risks relating to these technologies. Human vulnerability factors, such as compromised PINs, are not taken into account.

Principal Vulnerabilities of Mobile Devices

Vulnerability MD.1: *Untrustworthy Interface* In many cases, the security of an application boils down to the question as to whether a really trustworthy user interface exists (see *The Trusted Interface Problem* [1]). Since Trojans or viruses might attack mobile devices which have become as complex as PCs, this assumption cannot always be made. Besides that, the full range of browser-related vulnerabilities, eg, phishing, applies to mobile devices as well. However, in some of the use-cases described below we assume that the mobile device in general is more secure than an ordinary PC (eg, see Electronic Signature with Mobile Device (Trustworthy Viewing) below).

Vulnerability MD.2: *Theft/Loss of the Device* An additional vulnerability, which is rather uncommon in the desktop world but very serious when it comes to mobile devices (and laptops), is theft or loss of the device. Because mobile devices are very small and are usually carried around by their owners they get stolen or lost very often. A mobile device could somehow be used to verify an individual's identity but it should not contain the individual's identity because mobile phones are frequently lost or stolen.

Principal Vulnerabilities of Smart Cards

Vulnerability SC.1: *Physical Attacks* These kinds of attacks are usually invasive, eg, rewiring a circuit on the chip or using probing pins to monitor data flows. Physical attacks include altering the environment around the card, such as temperature or radiation, in order to induce faults. The goal of the attacker is to bypass security mechanisms and gain secret information stored on the card. In general, modern smart cards are quite resistant to physical attacks. Nevertheless, there have been a number of reverse-engineering attacks in attempts to retrieve private keys or find flaws in the hardware design.

Vulnerability SC.2: *Side-Channel Attacks* A more sophisticated attacker exploits additional physical information leaked through so-called side-channels during the execution of a transaction. This additional information could be the timing of signals, power consumption, or radiation. The usual counter-measures include the implementation of sophisticated software [23] and physical shielding.

The following two vulnerabilities do not relate only to smart cards but are nevertheless discussed here:

Vulnerability SC.3: ***Man-in-the-middle-attacks*** Even the best protection against physical attacks and an unbreakable encryption scheme do not help when the smart card cannot identify the party on the other side. Especially in the case of online authentication, where the communication is tunnelled via many hops, this vulnerability becomes a serious issue. The attacker inserts himself between the server and the smart card. Even if the channel is encrypted, both sides believe they are talking to each other, and the attacker can intercept, delete or modify the communications. The usual protection mechanism against this kind of attacks is mutual authentication.

Vulnerability SC.4: ***Cryptanalytic attacks*** These attacks directly target the cryptographic algorithms. Published algorithms are continuously being reviewed by the scientific community. Successful cryptographic attacks will, over time, lead to a need for greater key lengths.

Principal Vulnerabilities of NFC/Contactless Devices

There are numerous issues related to the use of NFC devices:

Vulnerability NFC.1: ***Skimming*** We speak of skimming when an unauthorized device secretly reads information from the device. For example, an attacker could obtain data from an unknowing end user who has the NFC/contactless device in his bag and who has placed the bag close to a hidden reading device. [9][11].

Vulnerability NFC.2: ***Eavesdropping*** The communication between two NFC/contactless devices can be eavesdropped from a certain distance [7][9][11][20]. In this case, the attacker would first record the communications from a close distance and later try to break the encryption (if any) with appropriate equipment. The most popular example for this vulnerability is a well-known weakness in the basic access control (BAC) mechanism deployed in electronic passports [13][17].

Vulnerability NFC.3: ***Tracking*** In many cases, NFC/contactless devices have a unique identification number (UID) which they send on request in order to establish a communication. This enables the movements of individuals to be tracked. Whenever the owner of a contactless device (eg, an NFC-enabled mobile phone) passes by an NFC reader (eg, integrated into the entrance gates of a big shopping mall), the monitoring system could store the UID in a database. Over time, a specific profile of the movements of the person would be created [1]. Of course, location tracking of mobile devices via the GSM interface is an important issue anyway, but is outside the scope of this paper.

Vulnerability NFC.4: ***Relay Attack*** Here an attacker cheats the local reading device through a communication link to a remote contactless device. Without any access control mechanisms it would be fairly easy to build a pick-pocket system that would secretly skim a victim's contactless smart card and run an authentication with a remote reader [15]. Basically, this is a man-in-the-middle-attack applied to NFC/contactless devices.

Vulnerability NFC.5: *Falsification of Content* The possible falsification of content due to unauthorised writing into the file system is a vulnerability. A manipulated UID could, for example, be accepted as authentic if there are no appropriate security measures in place [12].

Specific Use-Cases

From the above described 'general vulnerabilities' we can derive more 'specific vulnerabilities' for certain use-cases. In this section we describe some mobile eID use-cases which cover some of these specific vulnerabilities.

Downloading a Transport e-Ticketing Application to an NFC Mobile Phone Over-the-Air (OTA)

Use-case

Actors:

Customer, Mobile Network Operator (MNO), Transport Revenue Collector (TRC)

Scenario:

- **Customer sends a 'Download CityTransit Card' SMS to their MNO, or touches their NFC mobile phone to a 'Download CityTransit Card' NFC tag (at train station, bus stop, hotel lobby) which automatically sends the same SMS to their MNO.**
- **Mobile phone begins a download dialogue 'Would you like to download CityTransit Card with €10 value?'**
- **Customer confirms, MNO bills customer €10 to their mobile phone bill, debit or credit account and notifies the TRC to begin OTA download.**
- **TRC downloads CityTransit Card ticketing application to the customer's mobile phone over MNO network.**
- **TRC notifies MNO of successful download and bills MNO for €10. The billing and settlement does not necessarily include the application ID number of the CityTransit Card application or the mobile phone number of the mobile subscriber.**

Main vulnerabilities:

- **Fraudulent download of CityTransit Card (without paying or by charging another client's account)**

A customer can then make anonymous e-ticketing transactions using their NFC mobile phone (see next use-case).

Of course the customer may choose to personalise his or her CityTransit Card application if sufficient incentives are offered by the TRC. In this case there would be an additional Step 4.5 where the user will be required to input his or her national identity card number or social security card number to be transmitted OTA to the TRC.

Transport e-Ticketing Transaction Using NFC Mobile Phone

Use-case
Actors:
Customer, bus validator (software)
Scenario:
• **Customer places NFC mobile phone against a bus validator, when boarding a bus.** • **TRC validator software authenticates the CityTransit Card application.** • **CityTransit Card application on NFC mobile phone authenticates the bus validator.** • **TRC validator transacts with CityTransit Card application, deducts bus ticket fare from the balance in the application and writes a transaction record into the CityTransit Card application buffer containing the last transactions.** • **TRC validator stores the (offline) transaction and updated balance for this CityTransit Card application.** • **When bus returns to depot, the TRC validator software uploads transaction records back to the TRC clearing and settlement system[8].**
Main vulnerabilities:
• **Profiling and location tracking of passengers using the transaction records** • **Location tracking of passengers using secret reading devices** • **Unauthorized use of another passenger's Transit Card via a relayed connection (see below)**

For this use-case there exists a particular trade-off between convenience and security. If the service provider does not require the user to activate the device before the passenger pays the ticket by touching the validator with the mobile device (which would be very

[8] Assuming the use of the latest technology, this may also be done before the bus returns to the depot. We can expect the in-bus readers to have GSM or Wi-Fi connections and to be able to perform the download at different times during the day or at predetermined stops.

convenient for the customer), the system is particularly vulnerable to relay attacks. An attacker using two mobile devices, connected via a wireless connection (relay), would be able to pay tickets using the account of another passenger whose mobile device is located close to the attacker's reader.

Interactive Advertising (Smart Posters)

Use-case
Actors:
Customer, Provider
Scenario:
• **Customer taps NFC mobile phone against a smart poster** • **Poster sends information to the phone which can be used by the customer later on**
Main vulnerabilities:
• **Infection of the mobile device with viruses/Trojans via downloading multimedia files**

It should be mentioned that customer profiling is actually not a real vulnerability here. It is quite clear that collecting data about its customers is a business necessity for the service provider. However, this has to be properly communicated to the users.

There are several similar scenarios using location details – eg, interactive posters or GPS – to provide location dependent services.

Mobile Voting

A mobile phone can be used in voting procedures. These procedures could be anonymous online polls (eg, as part of TV shows), inter-company elections or even legally binding electronic voting [24]. In the latter cases (described below), the major challenges are assuring that eligible voters vote once and only once while the secrecy and anonymity of the vote are guaranteed.

Use-case
Actors:
Voter, voting office
Scenario:
• **After initialization, voters can enter into dialogue with the electronic ballot box** • **Similar to postal voting the actual vote is encapsulated in an encrypted electronic envelope** • **Encrypted vote is submitted to the voting service with anonymous voter's credentials** • **Voting service checks voter's eligibility and the vote is cast into the electronic ballot box** • **Electronic ballot box is opened for tallying the votes**
Main vulnerabilities:
• **Voters credentials are used by an non-eligible voter** • **Violation of voting procedures and of the clear separation into: initialization – voting/election – tallying – clean-up**

Electronic Signature with Mobile Device (Trustworthy Viewing)

A user, not necessarily permanently connected to the Internet, wants to sign electronically a document that he has received by e-mail. The user owns a particular private/public key-pair marked for this purpose. We assume that the legislation in user's country requires that the private key be stored on a smart card device in order to prevent repudiation of the signature. We furthermore assume that this smart card is (or can be) integrated into the mobile device.

Use-case
Actors:
User, PC application
Scenario:
• **User views document on desktop, wants to sign it and starts application** • **Application asks user to connect mobile device to PC** • **User sees document (or parts of the document) on the display of the**

mobile device[9]

- **User enters PIN at mobile device**
- **User receives signed document on desktop or mail account**

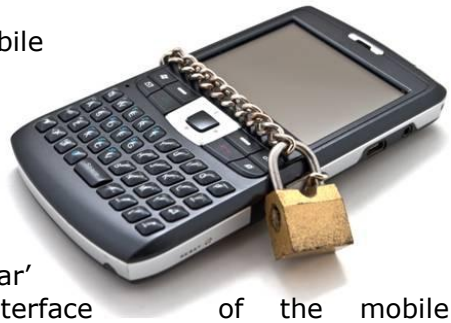
Main vulnerabilities:

- **Compromised viewer application (Trojan/virus)**

Under the assumption that the mobile device is more secure than the PC (see below), it adds to the overall security of the system. This idea is called 'splitting trust' [2]. The system is divided into two devices, one powerful and less secure, the other one more secure but less powerful; on each of these devices a part of the application runs, split up in a way that the combined system is powerful *and* more secure.

The assumption that the mobile device is more secure than the PC is based on the following aspects:

- Applications on the phone are in general less complex and therefore less susceptible to Trojan/virus attacks;
- Since there is a liability from the MNOs for mobile phones (in contrast to PCs), applications in general are more closed and security settings are tighter;
- The phone is more under the personal control of the user.



The advantage of this concept compared to a 'regular' smart card connected to the PC is therefore the trusted interface of the mobile device [1][22]. In the scenario where the smart card is directly connected to the PC, it is impossible for the user to see which document the smart card actually signs. Even if the smart card itself is secure and the access to the private key is protected with a secret PIN, a compromised PC application would still be able to display the document the user intends to sign but send a different one to the smart card for signing.

Online Authentication with National ID Card (Mobile Phone)

The user wants to open a bank account. A national ID card is required for this procedure in most countries. We assume that the user is legally registered as a citizen in his or her country. To receive the national ID card, usually a citizen has to present themselves in person at a local office of the government.

[9] Alternatively, the mobile device is used to later verify the digital signature. If the PC application had been compromised, the verification on the mobile device would fail and inform the user.

Use-case
Actors:
User, bank
Scenario:

• **User connects to an application server via Internet**
• **Server asks for authentication: 'ID card required'**
• **Authentication:**
  • **User places mobile phone on NFC reader and enters secret PIN at PIN-card terminal (or on the phone)**
  • **Server reads all necessary information from the user's mobile phone/ID card (via NFC/Internet connection)**

Main vulnerabilities:
• **Compromised mobile device/ID card**

There is a fundamental difference between government-issued and industry-issued credentials with regard to online applications. Assuming that they are mandatory or at least widely deployed, government-issued credentials can be used for the very first step of every online application, the *registration process*. Since the user is already in possession of the credential, no appearance in person is required. On the other hand, for banks providing secure physical tokens for online banking purposes, the client of the bank usually has to show up in person and provide some ID card, passport or similar, in order to register for the service and receive the token. All subsequent steps can then be undertaken by using the bank's token.

Some thoughts on mobile phones replacing national ID cards....

A mobile phone which acts as a national ID card is technically feasible; turning this concept into reality, however, is something which today seems far in the future. On the other hand, if we look at the speed with which passports have migrated from paper-only security documents to security documents with embedded contactless chips (around five years) then the idea of a NFC mobile phone containing a travel identity application, such as a passport, might not be that far away. Before that date we are likely to see NFC mobile phones containing frequent traveller or frequent-flier applications issued by airlines, airports and even possibly by government agencies (although such an application would not substitute for the passport application). There are already a number of border control agencies which have issued eGate cards to ensure that their own citizens, or frequent visitors, can be more quickly facilitated through a border.

Technically, if the phone contains an evaluated, government-issued smart card which can establish an end-to-end encrypted channel with the reading device, its trustworthiness could be verified even if the phone itself is completely untrustworthy. In fact, it does not

matter *where* the ID card is, as long as it can communicate via a secure channel with the verifying device[10]. It is important to keep in mind that the use of a single mobile device, which not only serves as a phone but also as ID card (and maybe bank and credit card), creates new risks with regard to identity theft because 'all the eggs are in one basket'.

Furthermore, governments, in many cases, have made identity cards compulsory but they would face a challenge in making mobile phones compulsory. A mobile device could somehow be used to verify an individual's identity but it cannot store the individual's identity locally because mobile phones are frequently lost or stolen (even though it is technically feasible to protect access to the secure element). The vast majority of consumers would simply elect not to carry their identity credential in their mobile phone. For that reason it makes sense to distinguish between (obligatory) national ID cards and more general 'citizen cards' which are government-issued but can only be used for particular identification purposes.

Threats and Remedies

According to www.dictionary.com a threat is *inter alia* 'an indication or warning of probable trouble' [27].

- Financial losses

The most obvious threat is of course the (threat of the) theft of sensitive data which, in extreme cases, might even entail identity theft. Stolen personal information as well as direct attacks on online applications can sometimes be expressed in terms of financial losses, eg, in the case of manipulated bank transfers or depleted pre-paid accounts. Ticket falsification or ticket duplication pose financial threats to a transport service provider or its customers (if the fraud reduces another client's balance). Usually, for the service provider, the latter case is even more harmful since it results in a loss of reputation.

- Privacy invasion

Mere privacy invasion, without financial consequences, is a threat in itself. With respect to mobile devices, location profiles are an important issue.

- Document fraud (government-issued documents)

A general threat when it comes to ID cards is document fraud, even if it is not based on one of the particular vulnerabilities we listed above. Consequently, European governments

[10] A mechanism similar to extended access control (EAC), which is deployed in European electronic passports and envisioned in some eID card specifications [9], could serve for this purpose.

have developed very secure ID documents with numerous physical and digital security features. Integrating these documents into mobile devices raises a lot of security issues. Physical security features, such as Guilloche techniques or holograms [4], must be replaced by appropriate digital counterparts. The personalization of ID cards usually takes place in highly-secure government-controlled buildings, whereas the personalization of mobile phones can be undertaken online or in a phone shop. A possible approach would be a government-produced SIM card which could then be used in mobile phones. Certainly, the combination of a mobile device with a national ID card would require the collaboration of several authorities: (local and central) government institutions, MNOs and banks.

The challenge of mixing government and commercial applications is demonstrated in Malaysia, where the (compulsory) national smart identity card also contains a separate contactless chip for transportation fares and ticketing. The operator of the automated fare collection scheme for transportation fares and ticketing also issues its own contactless transport card (which predates the issuance of national smart identity cards that contain the contactless transportation chip). Every month only around 1% of contactless transport card transactions are made by national smart ID cards containing the contactless transportation chip. Malaysian citizens have a natural concern for the safekeeping of their national smart ID cards, particularly since the government imposes a penalty for the loss of a card, and this is believed to be a significant factor affecting the low number of fare and toll-road transactions made with national smart ID cards that contain the contactless transportation chip. Furthermore, these cards contain two completely different authentication levels and users tend not to use a 'secure card' in a 'less secure environment' since they feel like they would disclose more personal details than necessary.

Conclusions

Looking at the Asian market, where there are many new applications for mobile devices, we expect that these technologies will, one way or another, also appear in Europe. Apart from opportunities to increase the security level of already existing applications through the use of mobile devices (eg, trustworthy viewing of documents to be signed) this change in the digital environment will bring new security and privacy risks. Mitigating these risks will in many cases require changes in legislation. Consider, for example, an electronic ID card stored in a mobile phone: the European Union, together with other countries, has already invested a lot of effort in preventing the unauthorized reading and tracking of electronic passports. Similar considerations will have to be taken into account for ID cards and, in the long run, also for ID applications and payment applications stored on mobile devices. This leads to our first recommendation:

Conclusion MOB.1: *Privacy Requirements* The European governments should define privacy requirements for these new emerging technologies. Expert groups containing stakeholders from industry and academia and led by government representatives should produce specific guidelines to support legislative changes with substantial material.

We suggest that the guidelines cover the following topics in detail:

- NFC Payment with Mobile Devices -- Privacy Requirements
- Non-Payment NFC Mobile Applications (eg, Smart Posters) -- Privacy Requirements
- National ID Cards stored in Mobile Devices -- Privacy Requirements
- Location traces re Mobile Devices -- Privacy Requirements

Conclusion MOB.2: *Global Standards* Globally accepted standards, not regional or local, should be used for telecommunications, data transfer, OTA downloading, security, and payments. Global standards are essential for business needs and can ensure a certain level of security. It is clear that data protection and privacy commissioners need to be involved in order to arrive at a global solution, and the commitment of governments in advocating such a solution and being early adopters is indispensable.

With respect to eID cards, there are currently several European Specifications [9] and interoperability is an issue here. The issue of eID interoperability is outside the scope of this paper but the specifications of the ID cards integrated into mobile devices should certainly follow a (standardized) specification for national eID cards.

Conclusion MOB.3: *Cryptography* Cryptographic mechanisms used for the authentication of mobile devices should be based upon open, peer-reviewed scientific research. Technical specifications should be published. Only a policy of 'full disclosure' will allow European society to evaluate the security of these new technologies.

Conclusion MOB.4: *The Use of Mobile Devices as Trusted Displays for Digital Signature* A mobile device which acts as a smart card reader with integrated display can add to the overall security of the system (PC plus mobile device) when a document has to be digitally signed.

Conclusion MOB.5: *Mobile Device as National ID Card* The full integration of a national ID card into a mobile device is still a vision in Europe[11] and it seems highly unlikely that a mobile device would constitute an individual's primary identity credential in the near future.

Conclusion MOB.6: *Personalization and Registration* The personalisation processes of mobile phones, payment cards and of national ID cards are fundamentally different. Only through intensive co-operation can MNOs, banks and national ID card producers solve this problem, ideally under the guidance of appropriate government institutions.

Conclusion MOB.7: *End-User Awareness* Mobile infrastructures implicitly assign an important security role to the mobile device owner. Anyone addressing a mobile infrastructure for any purpose (mobile banking, e-ticketing, mobile payments, etc) should also address the problem of training end-users about the correct usage of the device.

[11] Estonia has made the first steps in this direction [5].

Final Remarks

New mobile technologies and devices which are already very popular in Asia will also reach Europe within the coming years. Europe is now in the phase where there are business models that have to be agreed on and security criteria that have to be met. It is the time for government and industry to make decisions about the further development of mobile devices. Mobile services bring clear benefits to customers and, if deployed correctly, can also enhance the level of security of already existing applications.

Acronyms

2FA	Two-factor Authentication
3GPP	Third Generation Partnership Project
BAC	Basic Access Control
eID	Electronic Identity
EPC	Electronic Product Code
LTE	Long Term Evolution
NFC	Near Field Communication
MNO	Mobile Network Operator
PDA	Personal Digital Assistant
PIN	Personal Identification Number
RFID	Radio Frequency Identification
SE	Secure Element
SIM	Subscriber Identity Module
SMS	Short Message Service
TAN	Transaction Authentication Number
TRC	Transport Revenue Collector
UICC	Universal Integrated Circuit Card
UID	Unique Identification Number
USSD	Unstructured Supplementary Service Data
WiMAX	Worldwide Interoperability for Microwave Access

References

[1] *Anderson, Ross et al*: Security Engineering, Second Edition, 2008, Wiley Publishing Inc., ISBN 978-0-470-06852-6
[2] *Balfanz, Dirk; Felten, Edward W*: Hand-Held Computers Can Be Better Smart Cards, 1999, Eighth USENIX Security Composium, ISBN 1-880446-28-6, pp 15-23
[3] *BitDefender*, E-Threats Landscape Report, IT&C Security Course, January-June 2008
[4] *Council of the European Union*, Security Documents - Security features and other related technical terms, http://www.consilium.europa.eu/prado/EN/glossaryPopup.html
[5] *Estonia* Website of the Estonian Electronic ID Card, http://id.ee/
[6] *German Federal Office for Information Security (BSI)*: Technical Guidelines for the Secure Use of RFID (TG RFID), Subdocument 1: Application area 'eTicketing in Public Transport'
[7] *German Federal Office for Information Security (BSI)*: Messung der Abstrahleigenschaften von RFID-Systemen (MARS), Projektdokument 1: Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation, http://www.bsi.de/fachthem/rfid/Mars_Teilbericht_1Therorie.pdf
[8] *i2010,* Presidency conclusions, following the i2010 conference 'Building on i2010: Which services and networks for tomorrow?' http://www.ssi.gouv.fr/fr/actualites/i2010en.pdf
[9] *Naumann, Ingo; Hogben, Giles*: Privacy Features in European eID Card Specifications, Elsevier Network Security Newsletter; August 2008; ISSN 1353-4858; pp. 9-13
[10] *European Network and Information Security Agency (ENISA) in co-operation with Hilton, Jeremy; Burnap Pete; Tawileh, Anas*: Methods for the Identification of Emerging and Future Risks, November 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/EFR_Methods_Identification_200804.pdf
[11] *Eurosmart*, RFID technology security concerns: Understanding Secure Contactless device versus RFID tag, Oct. 2007
[12] *Jaap-Henk Hoepman, Johanneke Siljee*: Beyond RFID: the NFC Security Landscape; TNO Whitepaper, Oct. 2007
[13] *ICAO* Machine Readable Documents, Doc 9303, Machine Readable Travel Documents, http://mrtd.icao.int/
[14] *Jøsang, Audun; Al Zomai, Muhammed; Suriadi Suriadi*: Usability and Privacy in Identity Management Architectures, 2007
[15] *Kfir, Ziv; Wool, Avishai*: Picking Virtual Pockets using Relay Attacks on Contactless Smart card Systems
[16] *KPMG*, Mobile payments in Asia Pacific, 2007
[17] *Mayáš, Václav; Říha, Zdenek; Švénda, Petr*: Security of Electronic Passports, UPENET, UPGRADE European NETwork, Upgrade Vol. VIII, No. 6, Dec. 2007, http://www.upgrade-cepis.com/issues/2007/6/upg8-6Upenet.pdf
[18] *Mobey Forum*, Best Practice for Mobile Financial Services, Enrolment, Business Model Analysis, Version 1.0, 2008
[19] *Mobile UK Today*: Over £2.6bn worth of stolen mobiles for sale online, May 28, 2008, http://www.mobiletoday.co.uk/CheckMEND_report_stolen_mobile_phones.html

[20] *Tobergte, Wolfgang; Bienert, Renke*: NXP White Paper, Eavesdropping and Activation Distance for ISO/IEC 14443 Devices, 2007
[21] *Postbank*: iTAN and mTAN: Einfach sicherer, http://www.postbank.de/itan, captured Oct. 23rd, 2008
[22] *Roßnagel, Heiko*: Mobile Signatures and Certification on Demand, S K Katsikas, S Gritzalis and J Lopez (Eds.), Public Key Infrastructures, Springer, Berlin Heidelberg, 274-286, 2004
[23] *Ruhr-Universität Bochum, Chair for Embedded Security*: Side-Channel Cryptanalysis Lounge, http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html
[24] *Voutsis, Nico; Zimmermann, Frank*: Anonymous Code Lists for Secure Electronic Voting over Insecure Mobile Channels, in: Mobile Government – An Emerging Direction in E-Government, ed. Ibrahim Kushchu, IGI Publishing – Hershey – New York
[25] *Wikipedia*, Phishing, http://en.wikipedia.org/wiki/Phishing, captured Sep 9th, 2008
[26] *Wikipedia*, TAN, http://de.wikipedia.org/wiki/Transaktionsnummer, captured Oct 23rd, 2008
[27] *Dictionary.com,* Threat, http://dictionary.reference.com/browse/threat, captured Sep 10th, 2008