Mobile Qualified Electronic Signatures for Secure Mobile Brokerage

Heiko Rossnagel[1]

[1] Chair of Mobile Commerce and Multilateral Security,
Johann Wolfgang Goethe University Frankfurt, Gräfstr. 78,
60054 Frankfurt, Germany
heiko.rossnagel@m-lehrstuhl.de
http://www.m-lehrstuhl.de

Abstract. Despite a legal framework being in place for several years, the market share of qualified electronic signatures is disappointingly low. Mobile Signatures provide a new and promising opportunity for the deployment of an infrastructure for qualified electronic signatures. We that SIM-based signatures are the most secure and convenient solution. However, using the SIM-card as a secure signature creation device (SSCD) raises new challenges, because it would contain the user's private key as well the subscriber identification. Combining both functions in one card raises the question who will have the control over the keys and certificates. We propose a protocol called Certification on Demand (COD) that separates certification services from subscriber identification information and allows consumers to choose their appropriate certification services and service providers based on their needs. This infrastructure could be used to enable secure mobile brokerage services that can ommit the necessity of TAN lists and therefore allow a better integration of information and transaction services.

1 Introduction

In the directive 1999/93/EC of the European Parliament and of the Council [ECDir1999] legal requirements for a common introduction of electronic signatures in Europe were enacted. The directive sets a framework of requirements for security of technology used for electronic signatures. Based on certificates issued by certification authorities, which certify public keys for a person registered by a registration authority, electronic signatures can be created with a so-called "secure signature creation device" (SSCD), carrying the private keys of a person.

The EC-directive distinguishes between "electronic signatures" and "advanced electronic signatures" [ECDir1999]. An advanced electronic signature is defined as an electronic signature that meets the following requirements:

"(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain
under his sole control; and

(d) it is linked to the data to which it relates in such a
manner that any subsequent change of the data is
detectable;" [ECDir1999]

Certification Service Providers can issue certificates for advanced signatures that will be qualified if they meet the requirements of Annex I of the directive. Those advanced signatures with qualified certificates will be refered to in this paper as qualified signatures.

In Germany and Austria, the local implementation of the EC directive requires evaluation of the SSCD to be done against ITSEC E4 or CC EAL 4+ levels [FuFr2000]. For directory services, stringent 24/7 availability and durability is required. Revocation lists and other feasible technology must be available to all accepting parties of signed documents. The EU suggests the implementation of a public evaluation infrastructure under control of a government authority. Germany has already implemented a system of evaluation service companies, evaluation consulting companies and the Regulatory Authority for Telecommunications [RegTP2004] as the responsible government authority.

The deployment of signature card products focused so far on smart cards with evaluation against the requirements for lawful electronic signatures. Based on these, personal computer based signature applications have entered the market. These applications require smart card readers attached to the workstation, thereby preventing user mobility.

The market share of EC-directive conforming smart cards is disappointingly low, failing to meet any involved party's expectations. This has partly been blamed on the incompatibility and missing standards of existing products. Also the lack of customers prevents companies from investing in signature products. As a result almost no commercial usage for qualified electronic signatures exists. Consequently no customers seek to obtain signature products.

There are numerous activities trying to enlarge the potential consumer base like putting key pairs on national identity cards [FSEID2004]. Lately there have been some efforts towards mobile signatures [ETSI] [Raddic2004] and this approach might have a chance to break up the deadlock of missing customers and missing applications.

However, there are numerous problems to be solved, before qualified signatures can be created with a mobile device.

2 Mobile Signatures

Mobile signatures are electronic signatures which are created using a mobile device and rely on signature or certification services in a location independent telecommunication environment. They allow signatory mobility beyond fixed, secure desktop workstation with trusted, personal signing equipment [FrRaRo2003]. Although using mobile devices for signature creation has several shortcomings (e.g. display size, communication costs, limited computing power), the high market penetration of cell phones [GSM2004] and the mobility gained make this effort potentially successful and promising.

Two possible signing approaches in the mobile environment have been proposed in the past: signatures created in centralized signing server environments located at service providers like mobile network carriers; and electronic signatures created inside the signer's mobile device using a smart card.

2.1 Server Based Electronic Signatures

It has been shown in [Ross04] that server based mobile electronic signatures can not achieve the status of advanced electronic signatures [ECDir1999].

According to Art.2, 2(c) the signature has to be created by means that the signatory can maintain under his sole control [ECDir1999]. By giving away the users private key to store it on a server this premise can not be fulfilled [Ross04].

2.2 Client Based Electronic Signatures

Signatures can be created inside the mobile device using a secure signature creation device which has to fulfill the requirements of Annex III. Using a multiple smart card solution, the signature smart card, certified by a certification provider, is inserted into the mobile device which already contains the usual SIM-card. Therefore, the signature process takes place on the mobile device and the user is able to use basically any signature card available on the market. This can be achieved by either exchanging the SIM-card with the signature card (Dual Chip) or by having an additional chip card reader within the mobile device (Dual Slot). The first solution is very inconvenient for the signatory since he has to switch of the phone to exchange the cards for the signature creation and again to use the phone functionality. In the latter case a specialized mobile phone is required that has multiple smart card slots which almost none of the current mobile phones do.

It would also be possible to use a single smart card that contains the SIM telephone functions, as well as the secure signature creation device. This can be achieved either by leaving some free space on the SIM-card, on which the components of the signature creation device can be installed later on, or by shipping SIM-cards with preinstalled signature functionality that has to be initialized and activated.

We propose the usage of evaluated smart cards suitable for qualified electronic signatures which are extended by the SIM functionality and usable through a unified interface, e.g. with the USIM[1] specification TS 21.111 [3GPPSpec]. Another approach might be the migration and evaluation of USIM with a full WAP[2]/WIM[3] implementation for the purpose of lawful mobile signing [WAPF2004]. Evaluation must be car-

[1] Universal Subsriber Identity Module

[2] Wireless Application Protocol

[3] Wireless Identity Module

ried out with ITSEC or Common Criteria within an evaluation process similar to the evaluation summarized in [FuFr2000].

3 Challenges of SIM Based Signatures

Using a single smart card for both functionalities provides the most convenient solution for the signatory. He can sign documents and distribute them via communication services of his cell phone like GPRS[4] or UMTS[5]. To ensure that the requirements of Art.2 2(c) are met, it is necessary to provide some sort of reliable access control to the signature functions. The usual PIN used to control the access to the telephone functions is not sufficient, since users can keep their phones and SIMs unlocked for convenience. Like traditional signature cards, SIM-cards can be certified according to security evaluation criteria and are under control of the user.

However, using a single smart card for multiple purposes raises new questions and challenges. The SIM-card is issued by the telecommunication provider, while the SSCD is issued by a certification service provider. Combining both functions in one card raises the question who will have the control over the keys and certificates.

The simple solution is that the deploying carrier also initializes the signature secrets to act as a trust provider for their customers. This seems to be reasonable at first glance, since some of the european carriers already own and maintain trust centers (i.e. Deutsche Telekom), but there are several shortcomings, which make this approach unpractical.

First of all the customer wants to leave the store with his SIM-card right away, so he can use his mobile phone instead of waiting several weeks for the certification process to be completed. Furthermore, binding the keys to a carrier creates a great hindrance for the customer to switch to a cheaper carrier in the future. From the carriers point of view this would of course be a positive effect. From the customer's perspective, however, it would be much better to be able to choose freely between different certification service providers.

Also due to the lack of success of the signature market so far most providers probably do not want to invest in building and maintaining their own trust center to provide certification services. In addition, they don't want to change their distribution channels unless they expect an increase in revenue.

Therefore, a different solution for mobile signing and certification is needed, that allows separation of subscriber information and certification services.

4 Certification on Demand

The mobile operator could sell SIM-cards equipped with a key generator for one or more key pair(s) which can be used for the signing functionality. After obtaining the SIM-card from the mobile operator, the customer can then generate the keys and

[4] General Packet Radio System

[5] Universal Mobile Telecommunication System

activate the signature component and the public key(s) can be certified by any Certification Service Provider on demand.

Through the separation of the telephone functionality and the (possibly later) certification of the user's identity by a certification service provider, both functions can be sold separately and can be obtained from different providers.

The carrier will probably face increased costs for the signature capable SIM-card but can also expect increasing traffic caused by signature services. All distribution channels will remain unchanged.

Figure 2 illustrates the necessary steps for the distribution of the SIM-card and the certification process.

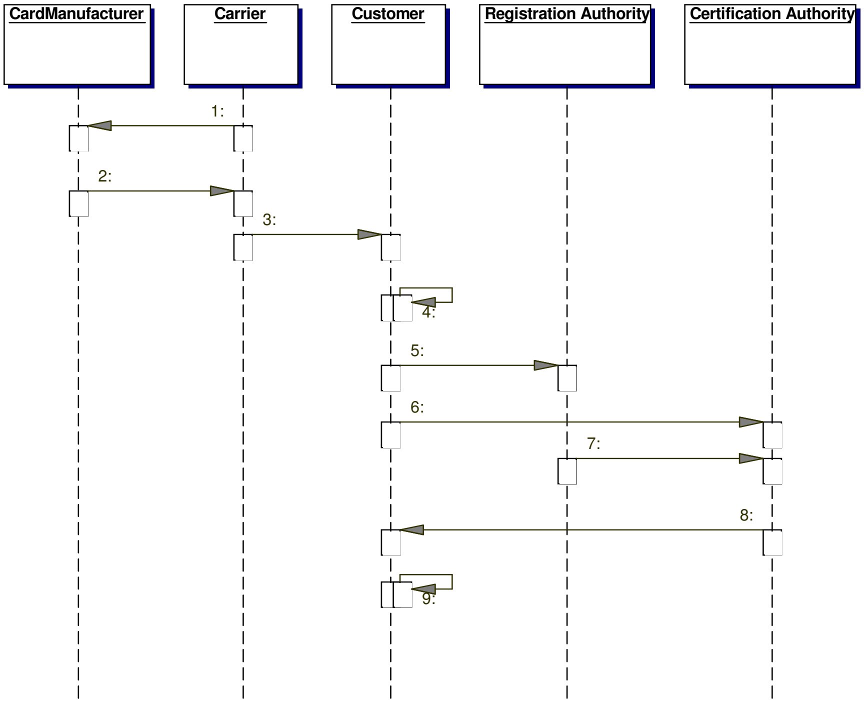

Fig. 1: Certification on Demand Protocol

1. The carrier gives his IMSI[6]/Ki[7] pairs to a card manufacturer.
2. The card manufacturer returns a SIM card containing an IMSI/Ki pair, a key generator for the signature application and the public key of the RootCA to the carrier.

[6] International Mobile Subscriber Identity

[7] Individual subscriber authentication key

3. The SIM card is sold to the customer and the carrier provides a nullpin that is used to generate the keys and activate the signing functionality.
4. The customer generates the keys and activates the signing functionality by entering the nullpin.
5. The customer registers at a Registration Authority of his choice, providing identification information and his public key.
6. The customer sends his identification information signed with his private key over the air to the Certification Authority.
7. The Registration Authority sends the public key and the identification information to the Certification Authority.
8. If the information provided by the customer and the Registration Authority match, the Certification Authority issues a certificate for the customer and sends it over the air to his mobile phone.
9. The user can verify the validity of his certificate by checking the certificate issued by the RootCA of the Certification Service Provider.

This protocol makes no changes to the existing distribution infrastructure of mobile operators. The steps 1 to 3 remain the same way they used to be before, apart from the fact that the card manufactures puts additional information and functionality (signature key generator, public key of RootCA) on the SIM card. In order to ensure that the card manufacturer does not know the private key of the user the key generation should be done by the card. The customer is not forced to certify his keys and can use the SIM for telephone functionality only. He could also activate the signing functionality without going through the certification process for example as a security token. If he wants to be able to make legal binding electronic signatures, he has to go through the complete process to obtain a qualified certificate. He can do this by freely choosing the CSP.

The nullpin to generate the keys and activate the signing functionality in step 4 is used to ensure that no signatures can be created before the customer has control over the SIM card. If the signature application has been activated before, the user will recognize this when entering the nullpin.

Step 6 could be omitted but serves as insurance for the customer to ensure him that the integrity of his identification information will be preserved.

If the customer wants to change his CSP, he only has to repeat steps 5 to 9 with his new CSP. If the customer wants to change his carrier, he has to go through the whole protocol again, but can register with his current Certification Service Provider.

5 Securing Mobile Brokerage

In recent years, financial services were expected as one of the key commercial drivers for the mobile commerce market [Forr2003]. As we know today, the market development of mobile financial services including mobile banking and brokerage services has not lived up to these expectations. Reconsidering the implementations of mobile financial services available, so far we can find that they are mostly reproductions of their (widely successful) web-based counterparts. This applies accordingly to the used security mechanisms. Consequently, they do not utilize their special features deriving from the mobility and infrastructural aspect. For example checking out the balance of accounts or requesting stock prices might be pastime but does normally not provide added value for customers and using transaction numbers for authorizing transactions while being on the way is inconvenient.

As research has shown [MuGu2004] [Munt2004] company announcements can have significant short term price effects on corresponding stock prices. If a private investor holds any stocks of the company, the portfolio value can be affected dramatically. As the resulting price effects can be very promptly and completed within a short time frame, investors should be notified and enabled to react immediately.

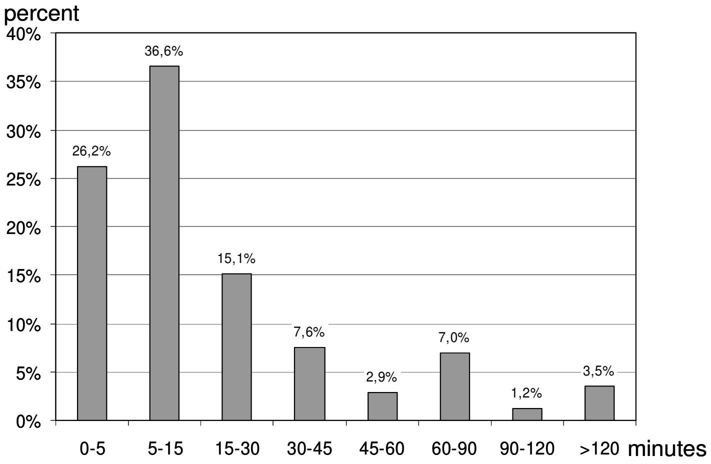

Fig. 2. Time conversion of the first five price fixings (n=172)

Figure 2 illustrates that nearly 80% of the first five price fixings can be observed within the first 30 minutes following the publication (arithmetic mean of 23.2 minutes). Therefore, an integration of mobile notification and transaction services, including prompt transaction authorization, is required if observed price effects persist for a short period of time only.

This can not be achieved with the traditional concept of online brokerage services.

An SMS message containing a relevant notification does not provide any protection of integrity or authenticity. A potential attacker will be able to pose as the news feed server sending false notifications.

Also it is very inconvenient for the investor to scan and enter a transaction number being pressed for time. Furthermore, the investor has to carry a list of TANs at all times in order to be able to react to incoming notifications. This increases the risk of potential theft or loss of the TAN list.

Using mobile signatures the integrity and authenticity of the notification can be checked by the investor. It also enables a secure integration of notification and trans-

action services providing authenticity and integrity for the transactions that are made by the investor.
A COD infrastructure allows financial institutions to certify and enable mobile subscribers to use banking services online through their mobile terminal and SIM. Credentials could be certified by the bank itself, like the credentials used on bank cards. Therefore, the bank can still have the control over the credentials while the mobile operator still can issue the SIM cards without giving their IMSI/Ki pairs away to the bank.

8 Conclusion

Mobile Signatures are a promising approach to break the deadlock between missing customers and missing applications. The high market penetration of mobile phones enables certificication service providers to target millions of potential customers. We analyzed two possible signing approaches (server based and client based signatures) and conclude that SIM-based signatures are the most secure and convenient solution. However, using the SIM as an SSCD seems to force the mobile operator to act as a trust provider and therefore to challenge the existing CSPs in a market that hasn't been successful so far. We proposed a protocol called Certification on Demand that seperates subscriber information from certification services and therefore enables both industries to cooperate instead of compete with each other.
This infrastructure could be used to enable secure mobile brokerage services that can ommit the necessity of TAN lists and therefore allow a better integration of information and transaction services.

References

[3GPPSpec] Specification of GSM, http://www.3gpp.org/ftp/Specs/archive/

[ECDir1999] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[ETSI] ETSI MCOMM Specialist Task Force 221

[FSEID2004] Project "Feasibility Study Electronic Identity Card", http:// www.uni-kassel.de/fb10/oeff_recht/english/projekte/projekteDigiPerso_eng.ghk

[Forr2003] Forrester Research, *European Mobile Forecast: 2003 To 2008*, Amsterdam, 2003.

[Fritsch2002] L. Fritsch.: A secure, economic infrastructure for signing of web based documents and financial affairs; CBL – Cyberbanking & Law, issue 2/2002;

[FrRaRo2003] L. Fritsch, J. Ranke, and H. Rossnagel: Qualified Mobile Electronic Signatures: Possible, but worth a try? In: Information Security Solutions Europe (ISSE) 2003 Conference, Vienna Austria

[FSMR2003] S. Figge, G. Schrott, J. Muntermann, and K. Rannenberg: EARNING M-ONEY – A Situation based Approach for Mobile Business Models; In: Proceedings of the 11th European Conference on Information Systems (ECIS) 2003

[FuFr2000] T. Fuchß, L. Fritsch: Security Certificates as a tool for reliably software engineering; Datenschutz und Datensicherheit 9/2000, pp.514ff.

[GSM2004] GSM Association: GSM Statistics www.gsmworld.com/news/statistics/index.shtml

[MuGu2004] J. Muntermann, A. Güttler: Mobile financial information services: Capabilities of suitable push services; Proceedings of the Eighth Pacific-Asia Conference on Information Systems (PACIS 2004); Shanghai, China

[Munt2004] J. Muntermann: Notifying Investors in Time - A Mobile Information System Approach; Proceedings of the Tenth Americas Conference on Information Systems (AMCIS'2004); New York, New York, August 2004

[Raddic2004] Radicchio, http://www.radicchio.org

[RaFrRo2003] J. Ranke, L. Fritsch, H. Rossnagel: M-Signaturen aus rechtlicher Sicht. In: Datenschutz und Datensicherheit 27 (2003) 2, p.95-100, Vieweg & Sohn

[Rann2003] K. Rannenberg: Identity Management in Mobile Applications In: Datenschutz und Datensicherheit 27 (2003) 9 (DuD), pp.546-550, Vieweg & Sohn

[RegTP2004] Regulierungsbehörde für Telekommunikation und Post (RegTP) der Bundesrepublik Deutschland; http://www.regtp.de/

[Ross2004] H. Rossnagel: Mobile Qualified Electronic Signatures and Certification on Demand, Proceedings of the 1st European PKI Workshop - Research and Applications, Springer LNCS 3093; Samos Island, Greece

[WAPF2004] WAP Forum: Specifications of WAP, WIM; http://www.wapforum.org/

[WiTness] European IST Project „Wireless Trust for Mobile Business“(WiTness), www.wireless-trust.org