Qualified Mobile Server Signature

Clemens Orthacker, Martin Centner, Christian Kittl

Qualified Mobile Server Signature

Clemens Orthacker[1] (clemens.orthacker@iaik.tugraz.at), Martin Centner[1] (martin.centner@iaik.tugraz.at), and Christian Kittl[2] (christian.kittl@evolaris.net)

[1] Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
[2] evolaris next level GmbH, Hugo-Wolf-Gasse 8/8a A-8010 Graz

Abstract. A legal basis for the use of electronic signatures exists since the introduction of qualified electronic signatures in EU Directive 1999/93/EC. Although considered as key enablers for e-Government and e-Commerce, qualified electronic signatures are still not widely used. Introducing a mobile component addresses most of the shortcomings of existing qualified signature approaches but poses certain difficulties in the security reasoning. The proposed server based mobile signature approach authenticates the signatory over trusted channels and assists the protection of the signature-creation data with organizational measures. As with traditional qualified signature approaches, strong authentication of the signatory to the system is ensured by two factors. Knowledge of a PIN and possession of a valid subscriber identity module card is verified over two separate communication channels. The qualified mobil server signature fulfills the requirements on secure signature-creation devices defined by the EU directive and in particular its Austrian implementation.

Keywords: qualified signature, mobile signature, signature legislation

1 Introduction

Advanced electronic signatures based on a qualified certificate and created by a secure signature-creation device, as defined in EU Directive 1999/93/EC on electronic signatures (see [1]) and referred to as *qualified signatures* in the following, are considered as key enablers in e-Government and e-Commerce. They provide a legal basis for transactions in online processes, while recognized standards for electronic signature formats ensure their seamless integration. However, qualified electronic signatures still lack wide-spread use in online applications and acceptance by citizens and customers. Three main factors for the low market penetration of qualified signatures have been identified in [14]:

1. Low dissemination of signature-creation devices
2. Lack of applications for electronic signatures
3. Shortfalls in existing business models

We propose a server-signature concept with the signature creation being triggered via the user's mobile phone. This mobile approach addresses the low dissemination of signature-creation devices since no costly smartcard readers are required. Even if in many EU member states qualified signatures on identity- or health insurance cards are available to a large public, the lack of card readers prevents them from being used as signature-creation devices. Further, introducing mobility addresses the lack of applications identified in [14] by opening up a new field for applications of electronic signatures. Finally, insufficient business models, mainly because of too high costs for the user, are not an issue if qualified certificates can be obtained free of charge.

Conformity of the proposed mobile server-signature concept with the requirements on secure signature-creation devices laid down in the EU directive on electronic signatures has been positively assessed in Austria. Signatures created in this way meet the requirements for qualified signatures as specified in the Austrian implementation [2] (SigG) and [5] (SigV) of the directive. Our proposal considers the Austrian signature legislation and does not necessarily translate directly to other national implementations of the directive.

A prototype of the proposed concept has been implemented by the authors. A further implementation has been provided and operated by an Austrian certification-service provider and is available to citizens for use in e-Government applications. We conclude that the Qualified Mobile Server Signature might be a valuable enabler for qualified signatures. Signature services triggered via mobile devices have already been proposed in [12], but have so far not provided qualified signatures.

Section 2 defines qualified signatures and introduces smart card based signatures as a traditional approach to qualified signatures. The combination of qualified signatures with mobile technologies is presented in Section 3 and Section 3.1 describes the proposed qualified mobile server signature scheme.

2 Motivation

2.1 Qualified Signature

Article 5, 1 of EU Directive 1999/93/EC [1] implicitly defines *qualified electronic signatures* as advanced electronic signatures based on a qualified certificate that are created by a secure signature-creation device and comply with the requirements in Annex I, II and III of the directive. Such signatures in relation to electronic data are considered legally equivalent to handwritten signatures on paper-based data. Moreover, they are admissible as evidence in legal proceedings. Almost all EU Member States have adopted this directive, the Austrian implementation comprises the *signature law* [2] (SigG) and the *signature ordinance* [5] (SigV).

Within the context of server signatures, the following parts of the directive are of special interest. The definition of advanced electronic signatures states in Article 2, 2(c) that advanced electronic signatures must be

> created using means that the signatory can maintain under his sole control.

Further, Annex III 1(c) requires secure signature-creation devices to ensure by appropriate technical and procedural means that

> the signature-creation data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

The Austrian signature law contains the sole-control requirement of Article 2, 2(c) literally in [2, §2 3.(c)]. Reliable protection of the signature-creation data of Annex III corresponds to the requirement on technical components to *reliably prevent the unauthorized use of the signature-creation-data* in [2, §18 (1)]. Apart from that, the Austrian signature law demands the signatory in [2, §21] to *carefully keep the signature-creation-data*.

The definition of advanced electronic signatures to be created using means the signatory can keep under his sole control, does not imply the use of special hardware as signature-creation device. Appropriate access control to the signature-creation data is sufficient, whereas Annex III in general requires the use of special hardware. Further, the requirements on cryptographic algorithms used for advanced electronic signatures are in general weaker than those derived from Annex III (see [3]). In this context, it seems therefore appropriate to focus on the fulfillment of the – harder – requirements of Annex III.

2.2 Traditional Qualified Signature Approaches

According to [1, Art.3.4] of the directive, a secure signature-creation device's conformity with Annex III shall be determined by appropriate public or private bodies designated by the Member States. To support these bodies, the Commission publishes reference numbers of recognized standards for electronic-signature products. Secure signature-creation devices are considered to conform with Annex III if they comply with one of these standards, which is however not a mandatory prerequisite. So far, the only published standard defining requirements for secure signature-creation devices in accordance with the directive is [8].

Many EU member states have already rolled out signature cards providing citizens with qualified signatures. These smartcards conform to the requirements of Annex III of the directive, in some cases due to their compliance with [8]. Usually, signature generation on such cards is protected by a personal (something the signatory knows) and a technical (something the signatory possesses) factor. In particular,the signatory has physical control over the card and can keep the signature creation PIN secret. Further, the signature-creation data is stored on the smart card only and it is technically assured that it cannot be read from the card's chip.

Reliable protection of the signature-creation data also involves protection of the data used to authenticate the signatory to the signature-creation device. For signature card approaches, [8] demands a trusted channel from the human

interface for pin-entry up to the device itself. Many SSCD implementations map this requirement on their environment to the responsibility of the user to utilize the signature card in a *trusted environment* only. Card readers with a pinpad help in assuring that the signature creation PIN is not intercepted by malicious software, but they cause significantly higher costs for the user and their use is not mandatory in many member states.

A major requirement for electronic signatures in e-Government is their seamless integration in online processes. Different approaches are employed to make card based qualified signatures available to (web) applications. A common solution is to provide users with a middleware for smart card access and abstraction. Applications communicate with this middleware via a defined high-level interface. Austria defines a webservice-like interface to a technology neutral signature-creation device ([10]).

Other conceivable implementations of secure signature-creation devices involve signature creation on mobile phones and server-signature services. Until now, there is however no published standard available to indicate conformity of such a solution to the requirements of the directive. [7], providing explanatory support for [8] however explicitly mentions the possibility to implement server signature or mobile phone based SSCDs.

3 Mobile Qualified Signatures

Combining qualified signatures with mobile technologies might open new fields of application for electronic signatures. Mobile signatures thus address the lack of applications identified in [14] as one of the reasons for the low usage for qualified signatures. For example, bank transactions effected on mobile devices with mobile TAN schemes are already widely adopted. Authorizing these transactions with qualified signatures would provide a better legal basis while providing a similarly high level of usability. The low dissemination of signature-creation devices, another major reason for the low market penetration of qualified signatures identified in [14], is not valid for mobile qualified signatures, neither.

Mobile signatures designate electronic signatures where at least the signatory employs a mobile device and at least part of the signature- or certification services is provided over a mobile carrier network (see [13]). The actual signature creation does not necessarily have to take place on the signatories handset. In general, client- and server based mobile signatures are distinguished, depending on where the signature is created.

Qualified signature creation on mobile devices requires dedicated cryptographic functionality and secure storage of the key on the subscriber identity module (SIM) card or a designated second card holding the signature-creation device. A software signature-creation application running on a mobile device does not fulfill the requirements of Annex III of the directive since (according to [7, Section 6.2.1]) at least part of the secure signature-creation device must reside in hardware in order to account for all possible threats on the signature-creation data. Embedding the signature-creation device on the SIM card requires integra-

tion of certification provider services within the mobile carrier's infrastructure. This has significant drawbacks for the user and yields organizational difficulties that mobile carriers are unlikely to be willing to take (see [14]). *Dual slot* devices on the other hand allow the separation of certification service provider and mobile carrier but are unfortunately not widely used.

Server based signatures are in general considered not to fulfill the requirements of Article 2, 2(c) of the directive. Advanced electronic signatures are required to be created by means the signatory can maintain under his sole control but with server based signatures, it is often claimed, the signatory obviously gives away control over the signature-creation data (see [13], [9]). Note however that the requirement for sole control does not imply the use of special hardware as signature-creation device (see [3]). Further, the authors of [4] argue that a suitable security concept and corresponding system configuration may allow the user of a server based signature service to maintain control over his key. In order to decide whether the security measures taken by such a service are sufficient, the signatory has to have access to a comprehensible version of the employed security concept and confidence that the service provider sticks to that security concept. The latter may be supported by a trusted auditor or supervisory authority.

The requirement of Annex III, 1(c) on secure signature-creation devices to reliably protect the signature-creation data implies a sufficiently strong authentication mechanism and the protection of the authentication data from the user interface to the signature-creation device (see [4]). Still, [7] states that the directive does not explicitly prohibit a server based signature-creation device. The protection profile defined in [8] however does not cover all relevant issues such as user authorization, user intentions and message display in such a system appropriately. In particular, trusted paths between the user interface, the signature-creation application and the signature-creation device have to be assured.

Accordingly, the Austrian signature law (SigG) lays down security requirements on technical components and processes where it requires the reliable prevention of unauthorized use of the signature-creation data ([2, §18 (1)]). The Austrian signature ordinance, governing the implementation of the Austrian signature law, however states in [5, §6 (3)] that

> in controlled surroundings, the security requirements on technical components and processes may be accomplished with organizational measures by using qualified and trustworthy personnel and by adopting adequate access control measures.

Designated bodies must confirm the fulfillment of these security requirements. Thus, organizational measures may assist in the fulfillment of the requirements of Annex III on secure signature-creation devices.

3.1 Mobile Server Signature

A SigG-compliant server signature may rely on organizational measures in combination with appropriate user authentication over trusted channels to meet

requirements on advanced electronic signatures of Article 2, 2(c) and on secure signature-creation devices of Annex III, 1(c).

We propose a server-signature concept, in the following referred to as *Mobile Citizen-Card*, that protects the signature-creation data by two factors. Similar to smart card based signatures, these comprise knowledge of a PIN. Unlike traditional qualified signature approaches, however, the technical factor *possession of a signature-card* is replaced by the possession of a registered subscriber identity module (SIM) card. The requirements on the signatory's local environment therefore reduce to a web browser for the communication with the server-signature application and an intact second communications channel via a mobile carrier network. There is no card reader or dedicated software needed on the client side.

The proposed server-signature concept relocates the secure signature-creation device from the signatories local environment to a server-side hardware security module (HSM). To compensate for this increased physical distance, the server-signature relies on two separate communication channels for performing the authentication of the signatory. The factor possession is ensured by relying on the mobile carrier network's ability to securely address a subscriber identity module.

3.2 Signature Creation

The server-side secure signature-creation device holds the signing keys of all registered users. Upon receipt of a signature creation request, the user is first prompted for a decryption-PIN to unlock the signature-creation data. At this stage the signature-creation data is still protected by the secure signature-creation devices's master key. A text message containing an authorization code is sent to the user's mobile phone. Only after the user has entered this authorization code on the server signature's web interface, the requested signature is created.

Given that hardware security modules are in general not able to securely store a large number of secret keys, the signing keys are protected as follows. A user's private *signing key* K_{sig}^{priv} is created onboard a hardware security module (HSM) and secured with a key-wrap algorithm using the system's AES master key MK. Since the master key is securely stored on the HSM and the key wrapping is performed on the HSM, the signing key never leaves the HSM unencrypted. It is further encrypted with a public key K_{user}^{pub} registered for the user within the system.

$$EK_{sig} = encrypt_{K_{user}^{pub}}(wrap_{MK}(K_{sig}^{priv})) \tag{1}$$

The private key K_{user}^{priv}, corresponding to K_{user}^{pub} is secured using AES in counter with CBC-MAC (CCM) mode (see [16]) with a decryption key derived (see [11]) from the decryption PIN, known only to the user.

$$K_{pin}^{sym} = derive(PIN) \tag{2}$$

$$EK_{user} = encrypt_{K_{pin}^{sym}}(K_{user}^{priv}) \tag{3}$$

EK_{sig}, EK_{user} and K_{user}^{pub} are stored within the system's database and retrieved with the user's registered mobile phone number. The decryption key K_{pin}^{sym} is

again derived from the user's pin-entry and used to decrypt the user's private key K_{priv}^{user}. Since this is done in CCM mode, the user key's authenticity and therefore the correctness of the PIN entered can be verified. Finally the wrapped signing key $EK_{sig,MK}$ can be retrieved and passed to the HSM for decryption and signature generation.

3.3 Security Considerations

The proposed server signature introduces TLS-secured trusted channels from the user interface to the signature-creation application and from the signature-creation device to the mobile carriers interface for sending text messages. The publicly available signature service introduces appropriate measures to avoid brute-force attacks on user's PIN, such as introducing delays or blocking the PIN. The signature-creation application and the signature-creation device are operated within a controlled environment and appropriate organizational measures are being taken to ensure a *trusted environment* for these parts of the server signature system. In particular, it is not possible for an attacker to obtain the decrypted (but still wrapped) key, pass it to the signature-creation device and sniff the generated authentication code. When transmitted to the signatory, the authentication code is protected by GSM security measures and returned back to the service via a TLS connection. GSM text message security constitutes probably the weakest link in the protection of the authentication data; several attacks on GSM encryption are known. Note that for the proposed server signature scheme, caller-Id spoofing is not an issue since the user does not actively send text messages.

In order to ensure the data to be signed (DTBS) is not altered after being transmitted to the signature-creation application, the digest value is sent to the user along with the authentication code and may be compared with the digest value displayed by the service. More powerful mobile devices may even calculate the digest value themselves from the DTBS obtained from the (authenticated) service.

It is within the responsibility of the user to verify the authenticity of the service's certificate in order to prevent an attacker from intercepting the authentication data and avoid man-in-the-middle attacks. Further, the signatory must carefully compare the digest values to prevent an attacker from altering the to be signed data. A comprehensible security concept of the server signature must be available to the signatory and confidence in the service operator must be established by an independent audit. Compared to the responsibility of the signatory to ensure a trusted local environment (free of malicious software) for smart card based qualified signatures these requirements do not seem too difficult to accomplish.

4 Conclusions

The proposed server-signature scheme fulfills the requirements laid down by [1] on qualified signatures and provides mobile signature experience by using mo-

bile one-time codes for authorizing the signature creation. The signature service relies on a combination of technical and organizational measures to accomplish the security requirements on components and processes and, in particular, the signature-creation data. While storage and application of the signature-creation data is secured by technical means, the signature service partly relies on organizational measures to authorize access to components. These measures assure that the signature-creation data can be reliably protected by the legitimate signatory against the use of others.

Similar to card based qualified signatures, the signature creation is protected by knowledge of a PIN and possession of a physical token. The signature-creation data stored on the server is secured with a decryption PIN, known to the signatory only, and the system's master key, both of which can be reliably protected by organizational measures. Unlocking of the master key requires the signatory to prove possession of his subscriber identity module (SIM) card. This involves a second communications channel, which compensates for the physical distance of the secure signature-creation device residing on the server part and the user interface on the client side.

A proof-of-concept prototype of the proposed server-signature concept has been implemented by the authors, based on the signature-creation middleware project MOCCA ([6]). Pursuing the proposed concept, a second implementation has been developed by an Austrian certification service provider and is being operated since November 2009. The service is publicly accessible for registration[3] and test-request submission[4]. This server based signature service has been determined by the Austrian assessment body A-SIT to be compliant with the requirements on secure signature-creation devices of Annex III. The results of this assessment are publicly available at [15]. Therefore, according to Article 3, 4 of the EU directive, the conformance of the proposed solution with Annex III has to be recognized by all EU Member States.

Since the service is operated by the only Austrian certification service provider issuing qualified certificates, no additional measures need to be taken to strengthen users' confidence that the operator sticks to the security concept (as requested in [3]).

Qualified certificates for use with this server signature are provided free of charge and the the signatory is not charged for mobile carrier services for the authorization text messages. The third major reason for the low market penetration of qualified electronic signatures, weak business models, therefore is not valid for this signature service. The mobile server signature approach accounts for all major shortcomings of qualified signature schemes identified in [14].

References

1. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, `http://eur-lex.`

[3] https://www.a-trust.at/mobile/

[4] https://www.a-trust.at/mobile/https-security-layer-request/test.aspx

europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML
2. Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), StF: BGBl. I Nr. 190/1999 (1999), http://ris.bka.gv.at:80/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003685, (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.)
3. Working Paper on Advanced Electronic Signatures (2004), http://www.fesa.eu/public-documents/WorkingPaper-AdvancedSignature-20041012.pdf
4. Public Statement on Server Based Signature Services (2005), http://www.fesa.eu/public-documents/PublicStatement-ServerBasedSignatureServices-20051027.pdf
5. Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008), StF: BGBl. II Nr. 3/2008 (2008), http://ris.bka.gv.at:80/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20005618
6. Centner, M., Orthacker, C., Bauer, W.: Minimal-Footprint Middleware for the Creation of Qualified Signatures. In: Proceedings of the 6th International Conference on Web Information Systems and Technologies. pp. 64 – 69 (2010)
7. Comité Européen de Normalisation (CEN): Guidelines for the implementation of Secure Signature-Creation Devices (Jun 2002), ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14355-00-2004-Mar.pdf
8. Comité Européen de Normalisation (CEN): Secure Signature-Creation Devices "EAL 4+" (2004), ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14169-00-2004-Mar.pdf
9. Fritsch, L., Ranke, J., Rossnagel, H.: Qualified mobile electronic signatures: Possible, but worth a try? In: Proceedings of Information Security Solutions Europe (ISSE) 2003 Conference. Vieweg Verlag, Vienna, Austria (2003)
10. Hollosi, A., Karlinger, G.: The Austrian Citizen Card, http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20040514/introduction/Introduction.en.html
11. Kaliski, B.: PKCS #5: Password-Based Cryptography Specification Version 2.0. RFC 2898 (Informational) (Sep 2000), http://tools.ietf.org/html/rfc2898
12. mobilkom austria AG & Co KG: Certificate Policy für A1 SIGNATUR Zertifikate für Verwaltungssignaturen nach E-Government-Gesetz (E-GovG) (2004), http://www.signatur.rtr.at/repository/csp-mobilkom-cp-a1signatur-13-20040423-de.pdf
13. Ranke, J., Fritsch, L., Roßnagel, H.: M-signaturen aus rechtlicher sicht (2003)
14. Roßnagel, H.: Mobile qualifizierte elektronische Signaturen. Ph.D. thesis, Goethe-Universität Frankfurt a.M. (2008)
15. Secure Information Technology Center – Austria (A-SIT): Sichere Signaturerstellungseinheit der A-Trust für die mobile Signatur bestehend aus HSM und HSM Server (2009), http://www.a-sit.at/pdfs/bescheinigungen_sig/1087_bescheinigung_mobile_signatur_final_S_S.pdf
16. Whiting, D., Housley, R., Ferguson, N.: Counter with CBC-MAC (CCM). RFC 3610 (Informational) (Sep 2003), http://tools.ietf.org/html/rfc3610