Published in „29. Smartcard Workshop Tagungsband“ Proceedings of 29th SmartCard Workshop, 20-21 February 2019, Darmstadt, Germany. pp. 219-231, Ed.: Ulrich Waldmann, Fraunhofer SIT Verlag, ISBN: 978-3-9813317-3-8

Qualified Remote Signatures – Solutions, its Certification, and Use

Authors – Herbert Leitold · Daniel Konrad

Abstract

Qualified electronic signatures appeared the late 1990s to early 2000s as a legally recognised equivalent to ink signatures. To implement it, smartcards have been a tool of choice for a decade. Around 2010 alternatives based on signing servers appeared. These in several cases quickly outperformed smartcard solutions regarding take-up and use. This paper discusses reasons for that like zero-footprint on the user device and better fitting the current mobile and always-online way we use the Internet. Starting from Austria which first introduced qualified remote electronic signatures in Europe we discuss the experience made. We complement this with describing alternative solutions that emerged later and became known to the authors from their duties in certifying solutions under the European Union eIDAS Regulation. Requirements for and experiences with such certification get explained. The authors compare certification of smartcard-based solutions with certifying server-signing and argue that for the former long-lasting experience with the technology allows for rigid approaches, whereas for the latter the dynamics of emerging technological solutions ask for some flexibility in the certification approach.

1 Introduction

Qualified electronic signatures are a vehicle to replace traditional hand-written signatures using electronic means. They started with first national signature laws like in Germany or in Italy in the late 1990s. The European Union (EU) soon leveraged this to the Single Market with the Signature Directive [SigD99]. It gave a basis for the legal recognition of electronic signatures throughout the EU. After more than a decade experience with the Signature Directive its successor, the Regulation on electronic identity, authentication, and trust services (eIDAS), led to an even higher degree of harmonisation of electronic signatures [eIDAS14].

Legal equivalence to ink signatures makes qualified electronic signatures a security tool. It, thus, is no surprise that the Signature Directive and later eIDAS have set strong security requirements for the components and services involved in creating qualified electronic signatures. A tool of choice to meet requirements of secure signature-creation devices (SSCD) have been smartcards for a decade. Smartcards as SSCD were pretty successful in some cases, like the electronic identity (eID) card in Estonia: e-Estonia reports that since its introduction in 2002 more than 500 million signatures have been created with about 1.3 million active eID cards. Other countries’ national projects started with similar ambition, but the actual uptake was often not as satisfactory. The Austrian citizen card project was launched in 2003 and had its first widely available smartcard tokens in 2005 with the health insurance card and also all bank cards becoming SSCDs. The actual activation of these tokens as signature-creation devices did, however, not exceed about 50 thousand out of (back then) 6 million bank cards or about 90 thousand out of 9 million health insurance cards. When comparing the two examples Austria and Estonia some reasons might be compulsory Estonian eID versus voluntary activation in Austria or early take-up by high-volume services like for online-banking in Estonia.

The qualified signature landscape in Austria changed significantly with the introduction of the mobile solution "Handy-Signatur" in 2010. It quickly outperformed the existing smartcard solutions both regarding uptake and use. Figure 1 below illustrates that by comparing the development of the mobile solution with the health insurance card "e-card". We have chosen these two solutions, as their registration channels, activation and free of charge use is the same and makes them comparable, as well as the services that can be used are almost the same.

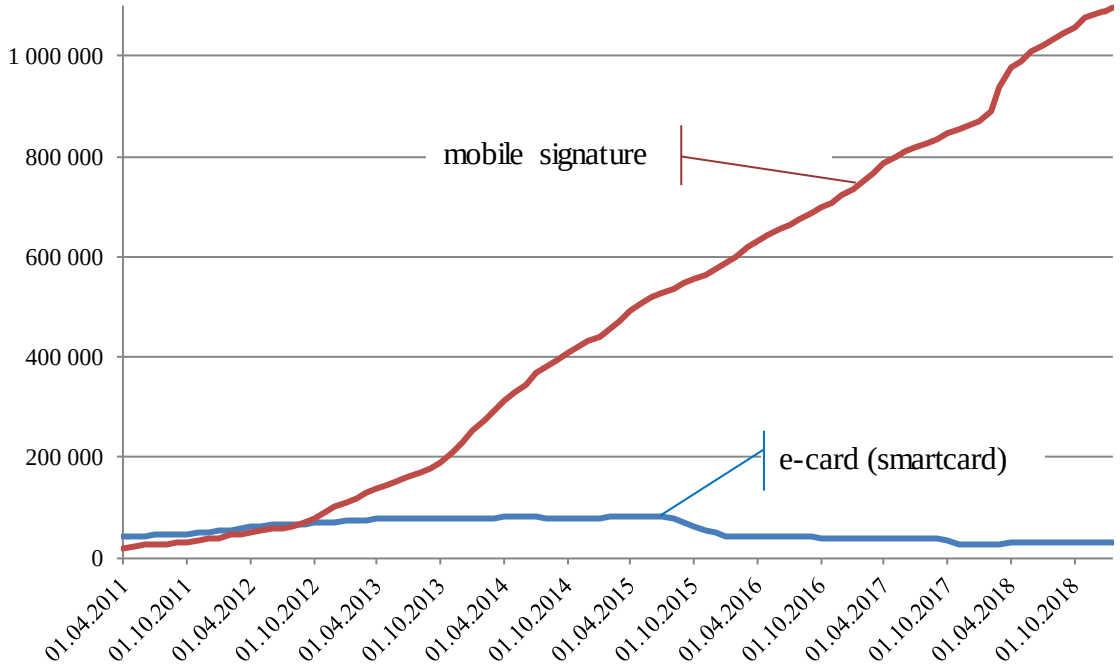

Fig. 1: Citizen Take-Up of Austrian Mobile Phone Signature versus Smartcard 'e-card'

The figure shows active SSCDs (the synonymous "QSCD" under eIDAS, respectively – cf. section 2) over time where mobile signature exceeds smartcards by far. Even when including all other Austrian smartcard SSCD tokens, like professions cards, that amount to about further 80 thousand (but are obligatory and therefore were not included in the figure, as it shall show citizen preferences under comparable situations) mobile outperforms smartcards by far.

We give experiences with remote signing solutions and how its characteristics influence certification as QSCD. Therefore, section 2 discusses the requirements for qualified electronic signatures. These are requirements for the qualified trust service provider (QTSP) issuing qualified certificates and conditions for the QSCD. This paper focusses on the latter, i.e. requirements for QSCDs. QTSPs are only touched when it is specific for our topic remote signature creation. Section 3 continues with case studies, which have been selected to illustrate aspects common to most services, but in particular differences concerning technical approaches are highlighted. We did choose the case studies from products that have been certified as QSCD by A-SIT, i.e. the authors learned during these certifications (note, that information in this paper is public in certification reports, we refrain from revealing background information or business secrets received). The experience made with certifications is discussed in section 4. This as remote QSCD certifications use a special eIDAS clause that currently allows for certification processes that are less harmonised than those for smartcard-type QSCDs. We argue that the flexibility given with this clause supports innovation in the early phases of emerging technologies like remote signatures are in. Finally, we conclude.

2 Requirements for Qualified Electronic Signatures

In this section, we discuss requirements for qualified electronic signatures that have been defined in the EU Signature Directive [SigD99], have later been revised with the EU eIDAS Regulation [eIDAS14], and compare these. Note, that for the main services or components involved the Signature Directive uses the terms "*qualified certification service provider (QCSP)*" and "*secure signature-creation device (SSCD)*", whereas eIDAS defines "*qualified trust service provider (QTSP) issuing qualified certificates*" and "q*ualified signature creation device (QSCD)*" for basically the same service or component. Even if largely synonymous, we stick with QCSP and SSCD whenever referring to the Signature Directive, QTSP and QSCD for eIDAS, respectively. We do so to keep the formally correct terms, but also to better distinguish requirements of the two legal acts.

2.1 Requirements under the Signature Directive

The Signature Directive defines that "… *advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device*" in relation to electronic data satisfy the legal requirements of handwritten signatures in relation to paper-based data (i.e., legal equivalence of electronic and handwritten signatures). We discuss requirements of the three parts advanced electronic signature, qualified certificate, and SSCD in this section. Given the overall topic of this paper, we emphasise on remote signing services.

An advanced electronic signature is a signature that is (a) *uniquely linked to the signatory*, (b) *capable of identifying the signatory*, (c) *created using means that the signatory can maintain under his sole control*, and (d) *linked to the data to which it relates in such a manner that any subsequent change of the data is detectable*. These legal requirements neatly fit the technical concept of a digital signature that serves data-origin authentication, i.e. it secures data (as described in (d)) and links this to the creator (provided by (a) and (b)). Requirement (c), however, is specific. While with a digital signature one would suggest that private cryptographic keys are somehow protected for its use by the signer only, the notion "sole control" was a source of debate and even confusion. It led to some argument that sole control can only be reached if the cryptographic keys are in physical possession of the signer, like with smartcard-type devices, and thus remote signing is ruled out by the Signature Directive anyhow. Such views, however, overshoot what was defined in the Signature Directive: In [FESA05] national supervision authorities stated that they "… *believe that sole control at least of the signature creation data can be achieved and that advanced electronic signatures can be created by a server-based signature service*" (with a dissenting note by the German supervision authority, stating that under German law sole control implies physical control). For Austria, the legislator in a 2007 amendment of the Signature Act, its explanatory notes and its bylaws clarified that sole control can be achieved by technical or organisational measures and is not constrained to physical control.

The requirement of a qualified certificate relates to a digital certificate being issued by a QCSP. Under the Signature Directive, this has no direct implication on remote signing services, we, therefore, do no further discuss QCSPs here. We just point to two aspects that we will later refer to in section 3.3 when comparing with eIDAS: The Signature Directive limits its scope to electronic signatures and services issuing certificates. Moreover, the Signature Directive does not mandate any ex-ante assessment of QCSPs – accreditation which would be such an ex-ante measure was voluntary.

Aside qualified certificates, the core security element defined in the Signature Directive was the SSCD. An SSCD needed to fulfil Annex III of the Signature Directive. To assess that,

Member States could designate national bodies. E.g., A-SIT, the organisation the authors of this paper are affiliated to, was the Austrian designated body. The requirements in Annex III were high-level, mainly that an SSCD had to ensure that signature-creation-data (i.e. private keys) (a) *can practically occur only once, and that their secrecy is reasonably assured*, (b) *cannot, with reasonable assurance, be derived*, and (c) *can be reliably protected by the legitimate signatory against the use of others*. These requirements to some extent mirror and extend what advanced electronic signatures define for the creation of electronic signatures. The Signature Directive did not mandate standards an SSCD has to meet. It, however, allowed for so-called reference numbers, i.e. standards where compliance with SSCD-requirements is to be assumed if a device meets such standard. Reference numbers have been settled in [ComD03].

The standards listed as reference numbers for SSCDs have been Common Criteria [ISO99] Protection Profiles [CEN02] that have been developed under the European Signature Standardisation Initiative (EESSI). When work in EESSI on defining standards for SSCDs started, the goal was to remain technology-neutral, but to at least be applicable to smartcards. This as smartcards those days were considered a tool of choice. Guidelines developed by EESSI on using these Protection Profiles [CEN04] discussed that these are also applicable to other user-held devices popular these days, like mobile phones or personal digital assistants (note, that smartphones as known today simply didn't exist). For remote signing services, these guidelines argued that such a service is quite possible, but saw some technical problems in applying the Protection Profiles to given hardware and software that existed back then. Those problems were not seen infeasible to solve, but the Guidelines saw the choices limited.

2.2 Requirements under eIDAS

The eIDAS Regulation introduces the term qualified electronic signature for a signature enjoying legal equivalence to handwritten signatures – a term that has been used before, even though it hasn't been defined under the Signature Directive. The eIDAS definition of a qualified electronic signature is the same as in the Signature Directive, i.e., an advanced electronic signature that is created by a QSCD and is based on a qualified certificate for electronic signatures.

The definition of an advanced electronic signature is – almost – a verbatim copy of the definition in the Signature Directive. A difference is that the clause that electronic signatures can be created using means the "*signatory can maintain under his sole control*" has been rephrased to "*the signatory can, with a high level of confidence, use under his sole control*". The addition "*with a high level of confidence*" might be read as weakening the requirement, given comparable requirements for SSCDs and QSCDs we argue that, what concerns certification of QSCDs, there is no practical difference.

eIDAS defines several trust services, like issuing qualified certificates for electronic signatures (of natural persons), qualified certificates for electronic seals (the equivalent to a signature by a legal person), qualified web authentication certificates (a Webserver-TLS-certificate with high-quality identification of the owner), timestamping services, signature or seal validation or preservation services, or services for registered electronic mail. A certificate for a qualified electronic signature is created by a QTSP where requirements are comparable to those in the Signature Directive. eIDAS, however, mandates an initial conformity assessment, which is an ex-ante evaluation against these requirements, followed by bi-annual periodic re-assessments.

With eIDAS remote qualified electronic signatures, i.e. using a QSCD that is not in physical control of the signatory, but uses private keys that are managed by a service provider on behalf of the signatory, are explicitly enabled. A requirement is that a QTSP operates the QSCD.

The requirements for QSCDs are laid down in Annex II of eIDAS; its core is phrased similarly to those in Annex III of the Signature Directive for SSCDs. The role of standards, however, changed: Once a standard for QSCDs has been published, this standard becomes mandatory for QCSD certification. Alternative certification by bodies designated by the Member States comparable to the situation under the Signature Directive is only permissible, if no applicable standard exists or if certification against such a standard is ongoing. In case such alternative certification is applied, the certification procedures used by the Member State designated body need to show comparable security levels and need to get notified to the European Commission.

Commission Decision [ComD16] sets QSCD certification standards. It defines Protection Profiles [CEN14] following Common Criteria [ISO99] and its Evaluation Methodology [ISO08] for QSCDs under physical control by the signatory, i.e. smartcard-like devices. For remote-signing QSCDs, however, no such standards have been listed. The argument given in recital (6) of [ComD16] is that no suitable standard existed. As we will further argue in the next section, with a standard listed for QSCDs becoming mandatory, amending [ComD16] needs to be done with caution not to disrupt an emerging market. Anyhow, with the current situation [ComD16] splits the QSCD certification landscape into two spheres: For smartcards and similar devices, a QSCD needs a Common Criteria certificate meeting [CEN14] (or at least an ongoing certification, which would allow for an interim alternative certification by a national designated body). The second sphere is remote-signing QSCDs where alternative certification schemes can be applied. To date, six Member States (Austria, France, Germany, Italy, Slovakia, and Spain) have notified such alternative schemes [Comm18].

2.3 Comparison of the Signature Directive and eIDAS

In this section, we summarise requirements for qualified electronic signatures by comparing requirements in the Signature Directive and in eIDAS. We start with general aspects and then focus on the particular scope of this paper – certification of remote-signing QSCDs.

What concerns electronic signatures, the most obvious difference between the Signature Directive and eIDAS is a much higher degree of harmonisation in the EU. This already is given with the superior legal instrument applied: The implementation of a Directive through national laws may differ between the Member States. See, e.g., the discussion on sole control in section 2.1, where [FESA05] has a dissenting note arguing that German law implies physical control, whereas Austrian law enables organisational and technical measures to implement it, but does not ask for physical possession. eIDAS as an EU Regulation, to the contrary, directly applies to each MS, thus no national law can create differences (still some national laws may be needed to implement the Regulation, or to clarify options – e.g., on electronic signatures temporary suspension of certificates is such an option a Member State may use).

A difference between the two legal acts also is that eIDAS explicitly allows for remote signing solutions. In its recital (52) eIDAS refers to remote electronic signatures as "*... set to increase in the light of its multiple economic benefits*". But eIDAS also recognises that compared with an entirely user-managed environment service providers need to take proper security measures. An implementation of such a rule is that a remote-signing QSCD has to be operated by a QTSP, i.e. a service provider that undergoes defined and recurring conformity assessments.

A difference in eIDAS specific to remote signing is that backup of private signature keys is allowed for service continuity, a situation disallowed and pretty unusual for smartcard-like signature devices: If a signatory's local QSCD is broken, replacing the smartcard with new signing keys is common practice. If a remote signing device managing many users breaks, renewing keys could mean re-enrolling thousands or millions of users (cf. section 1 on the Austrian "Handy-Signatur" currently having 1.1 million active users). As we will show in the case studies in section 3, remote signature solutions usually have a technical binding between the signature keys and the user's authorisation credential to have a strong sole control relation, which however would lead to such re-enrolments, if encrypted key backups would not ensure business continuity.

The higher degree of harmonisation also is based on the role of standards in eIDAS. When standards are referenced in Implementing Acts and Delegated Acts these (in most cases) become mandatory standards. An example is standards for QSCD certification: At first sight, the situation under the Signature Directive and its SSCD reference numbers [ComD03] looks similar to eIDAS and QSCD certification in [ComD16], as in both cases the legal act lists applicable standards. The subtle difference, however, is that the reference numbers under the Signature Directive were phrased as "maximum standard" in a sense that a producer could assume compliance with the Signature Directive if a certification against the Protection Profiles [CEN02] passed. Member States could not state additional, higher requirements, or the producer could undergo certification by designated bodies against Annex III of the Directive if it feels that [CEN02] does not suit the particular product well. On the other hand, standards listed under eIDAS like the Protection Profiles [CEN14] are "minimum standards" in a sense that products have to undergo a related certification. While the Member States still may not set requirements over these standards, the producer has no choice than to apply this standard (note, that parts 2 to 6 of [CEN14] have some variants and possible extensions, thus at least some degree of flexibility exists).

The current QSCD certification standards [CEN14] are primarily targeted at smartcard-like devices. Thus, the distinction in [ComD16] to mandate these standards for such devices, but not list standards for remote-signing QSCDs, is sensible. Meanwhile, comparable Protection Profiles for remote-signing QSCDs have been completed [CEN19]. With the "minimum standard" approach followed in eIDAS which makes a standard mandatory once listed in the Implementing Act, we argue that such inclusion has to be made with caution: The sole existence of a standard seems not yet justifying mandating it. The standard better first should proof being fit for purpose by showing market adoption and after several solutions certified against should show that it is applicable and making it mandatory does not disrupt the market. One might argue that the same line of thought could or should be applied to certification of smartcard-like devices, as well. A difference seen is that [CEN14] is an evolution of [CEN02] feeding in more than ten years of experience from certification under the Signature Directive, whereas [CEN19] for remote-signing QSCDs started from scratch and does not yet have such a long-term basis.

The actual scope of certification in eIDAS remained the same as in the Signature Directive. It is described in recital (56) of eIDAS that "… *should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device*". This is similar to recital (15) in the Signature Directive, but more explicitly limits the scope of certification to protecting the signature keys in the QSCD.

3 Case Studies

We base our discussion of remote-signing QSCDs and its environment to a very basic and simple architecture that is illustrated in figure 2 below. This simple schematic is used as it is an abstract view to all remote QSCD certifications we carried out. The right-hand side represents the environment the QSCD operates in. It usually consists of a hardware security module (HSM) that, following the scope defined in Annex II and considering recital (56) of eIDAS represents the QSCD. As an HSM is usually not capable of storing the number of signature-keys remote-signing solutions are designed for, the HSM may be complemented by a database keeping encrypted signature-keys while not in use (note, that some solutions create keys on demand for each electronic signature and use them just once). The system has a frontend to interface with users (signatories) and to applications the request documents to be signed (usually Web-applications).

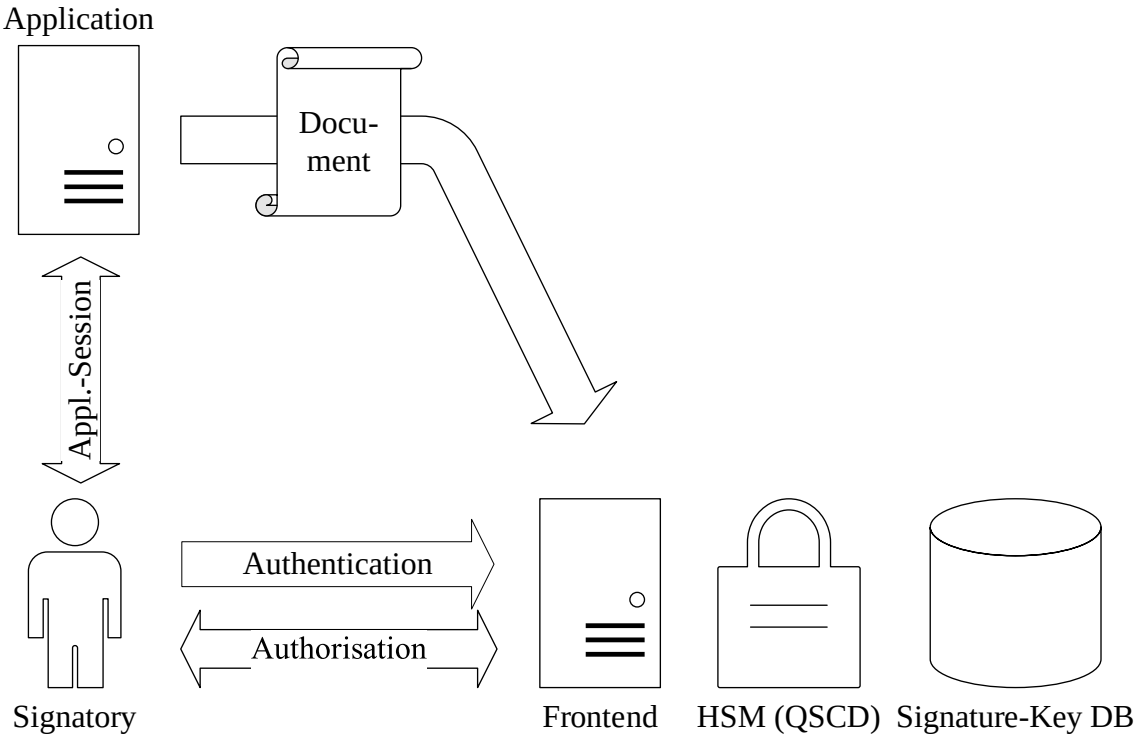

Fig. 2: General Schematic for Remote-Signing Solutions

The user has a session with an application that requires a document to be signed. This is usually a Web-application like an eGovernment site or an Internet-banking application. To create an electronic signature the user has to authenticate with the remote-signing service, and after inspecting that data to be signed to authorise the qualified electronic signature. In this general view, we deliberately do not show the user device, as – depending on the solution – this may need two devices or can be one device.

3.1 Austrian Mobile Phone Signature

The Austrian mobile phone signature "Handy-Signatur" has been developed as part of the EU Large Scale Pilot STORK in 2009 and went into production in 2010. The aim was to overcome low take-up of Austrian smartcard eID, but also to provide zero-footprint solutions that – aside from a Web browser – has no requirements on the user device. The latter as the advent of tablet computers with different business models did no longer allow for assumptions on us-

er environments, like USB interfaces to connect a smartcard reader, systems that would enable installation of specific drivers, or active elements like Java.

The mobile phone signature has been certified as SSCD under the Signature Directive and re-certified as QSCD under eIDAS [ASIT18a]. The core concept neatly fits figure 2 above: Signature keys are stored encrypted in a database when not in use. The encryption keys are constructed from an HSM key, the signatory's mobile phone number, and the signatory-chosen password. Thus, sole control by the user is implemented so that the HSM can only decrypt if the user is authenticated.

The authorisation of a qualified electronic signature is initiated by the HSM through creating a challenge and a verification code, both to be delivered to the signatory's mobile phone. The verification code is displayed by both the remote-signing service in the browser, and the signatory's mobile phone, it helps the users to associate a signature request to an application session. The way the verification code is transmitted, the challenge is transmitted and returned by the user, respectively, evolved:

- The first version used short message service (SMS) one time passwords (OTP). Signatories were advised to use two components for the Web application to authenticate and for receiving the SMS-OTP to ensure a two-component strategy to avoid that potential malware might succeed in compromising just a single device to get hold of both the password and the OTP.
- With the higher penetration of smartphones, an App and QR option was introduced. An app was provided for the major mobile operating systems that is paired with the user account at the signature service. The OTP gets presented to the user browser as a QR code and the user uses the app to take a photo. This enforces the two device approach, as the mobile phone camera needs to face a screen.
- The latest version makes use of the hardware secure element (SE) provided by modern smartphones. The mobile phone app pairs this SE cryptographically with the signatory's account at the signing service. An authorisation of a signature is through a PIN or biometrics with the SE.

With nowadays smartphones the third option is the default, provided that the phone has a hardware SE. It provides both higher security than the other options and convenience of use through the smartphones on-board methods like fingerprint sensors.

3.2 Different OTP Solutions

Soon after Austria introduced its qualified mobile signature similar solutions appeared in other countries. This may to some extent be attributed to the visibility of the success of the Austrian case, but certainly much more to similar demands like zero footprint solutions avoiding separate devices like smartcard readers, the emergence of tablets, or simply the mobile way we use the Internet.

The first such solutions were certified in 2015 as SSCDs under the Signature Directive and now have been re-certified as QSCDs under eIDAS [ASIT17a], [ASIT17b]. The architecture of these was almost identical to the one shown above and there was also a user-defined password needed for encrypting and activating the stored signature-keys. As a second authentication factor for activating the signature keys, an OTP mechanism is used and the QSCDs can be configured to address different widely used providers of OTP token solutions. The information about the OTP provider to be used and the respective OTP identifier is stored together with the encrypted signature key in the database. All cryptographic operations of generation, encryption and decryption of signature keys are implemented within the HSM and the appli-

cation of the signing keys within the HSM is only possible after a successful OTP validation and authentication with the signatory's secret password.

In addition to the integration of various OTP token solutions one QSCD vendor has also implemented a phone-call procedure and a biometric mechanism as second authentication factors [ASIT17c].

3.3 Delegated Authentication

With the definition of requirements for strong authentication mechanisms in Commission Implementing Regulation 2015/1502 [ComR15] and in the European Standard for Trustworthy Systems Supporting Server Signing [CEN18] ("SCAL2 – Sole control assurance level 2") some QSCD vendors implemented an option to completely delegate the authentication of the signatory to a trusted identity provider (IdP) [ASIT17c], [ASIT17d], [ASIT18b]. In such cases, the authentication factors are verified by an external IdP that issues an assertion and this assertion must be verified by the QSCD before the signing keys are activated. The IdP has to meet the authentication requirements for SCAL2, i.e. authentication means equivalent to Implementing Regulation 2015/1502 for assurance level substantial or high must be used. The QTSP that operates the QSCD is responsible for choosing appropriate IdPs and must verify that the IdP meets the requirements.

Note, that eIDAS does not create a dependency between QSCD requirements and eID levels of assurance in Regulation 2015/1502. The solutions described in this section used the eID requirements as a specification for authentication strength. An interesting aspect, however, is that an eID notified under eIDAS can then be used to trigger qualified electronic signatures without additional hardware on the user side, even if the eID itself does not support qualified signatures.

3.4 Short Time Keys

Some QSCD vendors [ASIT17e], [ASIT18c] implemented an approach slightly different from the architecture shown in figure 2 above. Here the signing keys are not stored persistently in encrypted form in a database but they are only temporarily created and available inside the HSM for the duration of a signing session. Upon completion of the signing operation, the key is destroyed inside the HSM and for any further signing session, a new key pair (and thus a new certificate) will be generated. Thus, it is not necessary to implement a database with encrypted signing keys. However, there is also a QSCD vendor [ASIT17c] that supports both approaches: persistent signing keys stored encrypted in a database as well as temporary signing keys used for a single session only.

4 Experience with QSCD Certification

What all the certified remote QSCD solutions have in common is that they use a certified HSM for the cryptographic operations. In fact, most of the solutions are using HSMs just from two different vendors. The respective HSMs are certified against either Common Criteria [ISO09] evaluation assurance level 4 (EAL4) or FIPS 140-2 level 3 [NIST01]. On the other hand, the signature activation mechanisms and the approaches to ensure the sole control requirement are varying greatly between the different solutions. The remote QSCD vendors need to quickly integrate new methods and technologies for the activation process, thus flexibility is required for the remote QSCD certification process. An example is different activation methods in the Austrian system that emerged from SMS-OTP to QR codes and then to employing hardware secure elements offered by nowadays mobile phones (cf. section 3.1).

Questions we received on certifications were how the operation of the remote QSCD fulfilling the conditions set in the QSCD certificate for secure operation is ensured. The process of certifying the component and setting conditions for secure use is in fact not different for remote QSCDs from smartcard-type devices. What is different is that eIDAS requires that a remote-signing QSCD needs to be operated by a QTSP. Thus, the implementation of secure operation can be enforced and checked during the QTSP conformity assessment: The QTSP operating the QSCD need not be a provider issuing qualified certificates for electronic signatures, but could, e.g., be a QTSP for timestamping services. In such a case, however, a further QTSP is needed that issues the related qualified certificates and that mentions the remote-signing QSCD in its certification practices. Thus, in any case, a QTSP is responsible for the QSCD it issues qualified certificates for and needs to ensure – either by operating the remote-signing QCSD itself or by contracting the QTSP doing the operation – that the QSCD is deployed as required. This becomes part of the conformity assessment QTSPs issuing qualified signature certificates have to undergo.

5 Conclusions

This paper described server-based remote solutions for qualified electronic signatures. Such solutions started complementing smartcard-like approaches from about 2010 when Austria introduced the first such product in Europe. This and some similar solutions by French and Italian vendors have been certified as SSCD under the regime of the Signature Directive, the products do benefit from a transitional measure in the eIDAS Regulation, thus are also QSCDs under this regulation.

With eIDAS explicitly enabling remote signing solutions a further boost has been seen. As of January 2019, a list of QSCDs maintained by the European Commission [Comm19] gives thirteen different remote-signature QSCDs that have been certified under eIDAS (in addition to SSCDs using transitional measures as mentioned before). Seven of these thirteen solutions have been certified by A-SIT (from vendors from Austria, Denmark, France, Luxemburg, and Italy) and involving authors of this paper. These seven products have been sketched here. Four further QSCDs have been certified by the Italian, as well as one each by the Spanish and the Slovakian certification body.

We argue that reasons for such a quick emergence of solutions are that remote signing services give advantages for the user, as it gives fewer requirements on the user side: Most solutions just require a browser and a mobile phone, some are prepared for just using the mobile phone. Further advantages we see are related to the central management of keys: Loss of a user device may lead to compromise of signature authorisation mechanisms, but not to loss of the private key. Once the loss of the device is detected, keys can be permanently destroyed. The same applies to compromise of cryptographic algorithms or keys, like it happened for smartcards with the ROCA attack [NSS+17]. While similar incidents cannot be excluded for HSMs, centralised key management eases mitigation. The centralised creation of signatures also gives implicit proof of existence, i.e. evidence that a certificate existed and was valid the very moment signature-creation is claimed in the signature (note, that the signing time is inserted by the remote signature server). This would allow reconsidering current revocation mechanisms like certificate revocation lists (CRLs) or online certificate status protocol (OCSP). Still, most remote-signing solutions continue using such revocation information in certificates for compatibility with existing signature verification tools.

Regarding certification of remote-signature QSCDs we saw similarities in the products, like all solutions relying on HSMs for the security-critical operations on cryptographic keys, i.e. for key generation, key use, and (if needed) for encrypted key storage. However, solutions al-

so followed different approaches, mainly in the authentication needed to initiate signature-creation. With remote-signature solutions also targeting mobile users and given the technological progress and dynamics in particular in mobile technologies we would assume seeing further innovative approaches in the near future. We argue that certification methodologies need to take that into consideration. While certification certainly shall not make a compromise on the assurance associated with a QSCD certificate, it also shall not hamper innovation. Therefore, the certification methodology needs to be flexible enough to incorporate new technological approaches. Regarding this, we see some difference in smartcard-type QSCDs and remote-signature QSCDs: There is a long experience in certifying smartcards as a relatively stable technological approach. This allows for descriptive standards on requirements. Remote-signing QSCDs, however, are rather new. We saw vendors adapting and amending products rather quickly. This asks for more flexibility in the methodology. The Commission Decision on QSCD certification [CommD16] implements this difference by setting minimum standards for certifying smartcard-type devices, whereas certification bodies can apply alternative methods for remote signature devices, as long as comparable security is ensured.

References

[ASIT17a] A-SIT: QSCD certificate “Qualified Signature and Seal Creation Device (QSCD) Intesi PkBox, Version 3.3”, 2018

[ASIT17b] A-SIT: QSCD certificate “Qualified Signature and Seal Creation Device (QSCD) AliasLab CryptoAccelerator, release 3.5.1”, 2017

[ASIT17c] A-SIT: QSCD certificate “Qualifizierte Signatur- und Siegelerstellungseinheit (QSEE) PrimeSign Remote Signing Device/Core für qualifizierte Signaturen und Siegel (QRSD-C, Version 1.0)“, 2017

[ASIT17d] A-SIT: QSCD certificate “Qualified Signature and Seal Creation Device (QSCD) LuxTrust’s Qualified Remote Signature and Seal Creation Device, version 1.0”, 2017

[ASIT17e] A-SIT: QSCD certificate “Qualified Signature Creation Device (QSCD) Protect & Sign, version 4.18”, 2017

[ASIT18a] A-SIT: QSCD certificate “Qualifizierte Signaturerstellungseinheit (QSEE) der A-Trust für die Handy-Signatur bestehend aus HSM und HSM Server, Version 1.3”, 2018

[ASIT18b] A-SIT: QSCD certificate “Qualified Signature and Seal Creation Device (QSCD) Cryptomathic Signer, version 4.8”, 2018

[ASIT18c] A-SIT: QSCD certificate “Qualifizierte Signatur- und Siegelerstellungseinheit (QSEE) des Swisscom All-in Signing Service (AIS), Version 2.3.1“, 2018

[CEN02] European Committee for Standardization: Secure Signature-Creation Devices Protection Profile EAL4+, CEN Workshop Agreement CWA 14169, 2002

[CEN04] European Committee for Standardization: Guidelines for the implementation of Secure Signature-Creation Devices, CEN Workshop Agreement CWA 14355, 2004

[CEN14] European Committee for Standardization: Protection Profiles for secure signature creation device, European Norm EN 419 211 Parts 1 to 6, 2013 and 2014

[CEN18] European Committee for Standardization: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements, EN 419241-1, 2018

[CEN19] European Committee for Standardization: Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, EN 419 241-2, 2019

[ComD03] European Commission: Commission Decision 003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, 2003

[ComD16] European Commission: Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 [eIDAS14], 2016

[Comm18] European Commission: List of alternative processes notified to the Commission in accordance with Article 30.3(b) and 39.2 of the eIDAS Regulation (EU) No 910/2014, version of 25/04/2018

[Comm19] European Commission: Member States' notifications on Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31(1)-(2), and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014, and information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014 [eIDAS14], version of 15/01/2019

[ComR15] European Commission: Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 [eIDAS14], 2015

[eIDAS14] European Union: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014

[FESA05] Forum of European Supervisory Authorities for Electronic Signatures (FESA): Public Statement on Server Based Signature Services, 17 October 2005

[ISO99] International Organization for Standardization, International Electrotechnical Commission (ISO/IEC): Information technology - Security techniques: Evaluation criteria for IT security, ISO/IEC 15408, 1999 (version applicable for [ComD03] and [CEN02])

[ISO08] International Organization for Standardization, International Electrotechnical Commission (ISO/IEC): Information technology - Security techniques: Methodology for IT security evaluation, ISO/IEC 18045, 2008

[ISO09] International Organization for Standardization, International Electrotechnical Commission (ISO/IEC): Information technology - Security techniques: Evaluation criteria for IT security, ISO/IEC 15408, 2009 (version applicable for [ComD16] and [CEN14])

[NIST01] National Institute of Standards and Technology: Federal Information Processing Standards Publication FIPS PUB 140-2 – Security Requirements for Cryptographic Modules, 2001

[NSS+17] Nemec M., Sys M., Svenda P., Klinec D., and Matyas V.: The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2017

[SigD99] European Union: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999

Herbert Leitold

CV

Herbert Leitold received a MSc. in telecommunication and informatics at Graz University of Technology in 1996, he then was research assistant at the same university. In 2002 Herbert joined A-SIT as Head of Unit Technology Assessment. In 2005 he became Secretary-General of A-SIT and Head of Unit Technology and eGovernment. Herbert is member of the Austrian delegation to the eIDAS Expert Group and the eIDAS Cooperation Network.

Contact

Herbert Leitold
A-SIT, Secure Information Technology Center - Austria
Inffeldgasse 16a
8010 Graz, Austria
Tel. +43 316 873 5521
E-Mail: Herbert.Leitold@a-sit.at

Daniel Konrad

CV

Daniel Konrad received a bachelor of science in telecommunication and informatics at Graz University of Technology in 2001. He joined A-SIT in 2001 where he is Head of Unit Inspections, Payment Systems, Certification, and Awareness. The duties of this unit include conformity assessments of qualified trust service providers and certifications of qualified signature creation devices under the eIDAS Regulation.

Contact

Daniel Konrad
A-SIT, Secure Information Technology Center - Austria
Seidlgasse 22/9
1030 Wien, Austria
Tel. +43 1 5031963 50
E-Mail: Daniel.Konrad@a-sit.at